

# Encoding Cardinality Constraints using Generalized Selection Networks

Michał Karpiński, Marek Piotrów

Institute of Computer Science, University of Wrocław  
Joliot-Curie 15, 50-383 Wrocław, Poland  
`{karp,mpi}@cs.uni.wroc.pl`

**Abstract.** Boolean cardinality constraints state that at most (at least, or exactly)  $k$  out of  $n$  propositional literals can be true. We propose a new class of selection networks that can be used for an efficient encoding of them. Several comparator networks have been proposed recently for encoding cardinality constraints and experiments have proved their efficiency. Those were based mainly on the odd-even or pairwise comparator networks. We use similar ideas, but we extend the model of comparator networks so that the basic components are not only comparators (2-sorters) but more general  $m$ -sorters, for  $m \geq 2$ . The inputs are organized into  $m$  columns, in which elements are recursively selected and, after that, columns are merged using an idea of multi-way merging. We present two algorithms parametrized by  $m \geq 2$ . We call those networks  $m$ -Wise Selection Network and  $m$ -Odd-Even Selection Network. We give detailed construction of the mergers when  $m = 4$ . The construction can be directly applied to any values of  $k$  and  $n$ . The proposed encoding of sorters is standard, therefore the arc-consistency is preserved. We prove correctness of the constructions and present the theoretical and experimental evaluation, which show that the new encodings are competitive to the other state-of-art encodings.

## 1 Introduction

Several hard decision problems can be efficiently reduced to Boolean satisfiability (SAT) problem and tried to be solved by recently-developed SAT-solvers. Some of them are formulated with the help of different high-level constraints, which should be either encoded into CNF formulas or solved inside a SAT-solver by a specialized extension. There was much research on both of these approaches.

In this paper we consider encodings of Boolean cardinality constraints that take the form  $x_1 + x_2 + \dots + x_n \sim k$ , where  $x_1, x_2, \dots, x_n$  are Boolean literals (that is, variables or their negations) and  $\sim$  is a relation from the set  $\{<, \leq, =, \geq, >\}$ . Such cardinality constraints appear naturally in formulations of different real-world problems including cumulative scheduling [16], timetabling [4] or formal hardware verification [8].

In a direct encoding of a cardinality constraint  $x_1 + x_2 + \dots + x_n < k$  one can take all subsets of  $X = \{x_1, \dots, x_n\}$  of size  $k$  and for each of them construct

a CNF formula that states that at least one of the literals in the subset must be false. The direct encoding is quite efficient for very small values of  $k$  and  $n$ , but for larger parameters another approach should be used.

**Related work:** In the last years several selection networks were proposed for the encoding cardinality constraints and experiments proved their efficiency. They were based mainly on the odd-even or pairwise comparator networks. Codish and Zazon-Ivry [9] introduced pairwise selection networks that used the concept of Parberry’s pairwise sorting network [15]. Abío, Nieuwenhuis, Oliveras and Rodríguez-Carbonell [1,3] defined encodings that implemented the odd-even sorting networks by Batcher [6]. In [1] the authors proposed a mixed parametric approach to the encodings, where the direct encoding is chosen for small sub-problems and the splitting point is optimized when large problems are divided into two smaller ones. They proposed to minimize the function  $\lambda \cdot \text{num\_vars} + \text{mun\_clauses}$  in the encodings. The constructed encodings are small and efficient, but non-trivial extra time is needed to find the optimal splitting points.

**Our contribution:** Partially inspired by this optimization criterion we started looking for selection networks that can be encoded with a smaller number of auxiliary variables and, if possible, not much larger number of clauses, and where there is no need for the costly optimization. In addition, we investigate the influence of our encodings on the execution times of SAT-solvers to be sure that the new algorithms can be used in practice. The obtained constructions are presented in this paper. The main idea is to split the problem into  $m$  sub-problems, recursively select elements in them and then merge the selected subsequences using an idea of multi-way merging [7,11]. In such approach we can use not only comparators (2-sorters) but also  $m$ -sorters, which can be encoded directly.

Using this generalized version of comparators we have created two novel classes of networks parametrized by  $m \geq 2$ . First one is called  **$m$ -Wise Selection Network**, in which we use the idea of pairwise sorting [15] combined with a multi-way merging algorithm by Gao, Liu and Zhao [11], but in more general way. The second class is called  **$m$ -Odd-Even Selection Networks**, where the multi-way merge sorting networks by Batcher and Lee [7] are generalized in a way that we can recursively select  $k$  largest elements from each of the  $m$  sub-problems. It should be also pointed out that none of the algorithms presented in this paper is using or is even based on the construction presented in the CP’15 paper of Karpiński and Piotrów [12]. The reason is that there the size of an input sequence is required to be a power of 2.

Both algorithms are presented using divide and conquer paradigm. The key to achieve efficient algorithms lie in the construction of networks that combines the results obtained from the recursive calls. The construction of those *mergers* is the main result of this paper. We fix  $m = 4$  and give detailed constructions for two merging networks: 4-Wise Merging Network and 4-Odd-Even Merging Network. We prove their correctness and compare the numbers of variables and clauses of the corresponding encodings to their two counterparts: Pairwise Merging Networks and Odd-Even Merging Networks [9]. The calculations show that

encodings based on our merging networks uses less number of variables and clauses, when  $k < n$ . In case of 4-Odd-Even Merging Network this also translates into smaller encodings in terms of variables and clauses for the 4-Odd-Even Selection Network in comparison to Odd-Even Selection Network, for sufficiently large  $k$  and  $n$ .

The constructions are parametrized by any values of  $k$  and  $n$ , so they can be further optimized by mixing them with other constructions. For example, in our experiments we mixed them with the direct encoding for small values of parameters. We used the standard encoding of  $m$ -sorters, therefore the arc consistency is preserved. Finally, we present results of our experiments, which is another main contribution of this paper. We show that generalized selection networks are superior to standard selection networks previously proposed in the literature, in context of translating cardinality constraints into propositional formulas. We also conclude that although encodings based on pairwise approach use less number of variables than odd-even encodings, in practice, it is the latter that achieve better reduction in SAT-solving runtime. It is a helpful observation, because from the practical point of view, implementing odd-even networks is a little bit easier.

We also empirically compare our encodings with other state-of-art encodings, not only based on comparator networks, but also on binary adders and binary decision diagrams. Those are mainly used in encodings of Pseudo-Boolean constraints, but it is informative to see how well they perform when encoding cardinality constraints.

**Structure of the paper:** The rest of the paper is organized as follows: Section 2 contains definitions and notations used in the paper. In Section 3 the construction of the generalized selection networks and the proofs of correctness are given. Section 4 is devoted to specialized merging networks for  $m = 4$  and contains detailed proofs of correctness. In Section 5 we compare the encodings produced by the construction with Pairwise Cardinality Network and Odd-Even Selection Network, in terms of number of variables and clauses each of them uses. Our experimental evaluation is presented in Section 6 followed by Conclusions.

## 2 Preliminaries

In this section we introduce definitions and notations used in the rest of the paper. Let  $X$  denote a totally ordered set, for example the set of natural numbers  $\mathbb{N}$  or the set of binary values  $\{0, 1\}$ . We introduce the auxiliary "smallest" element  $\perp \notin X$ , such that for all  $x \in X$  we have  $\perp < x$ . Thus,  $X \cup \{\perp\}$  is totally ordered. The element  $\perp$  is used in the next section to simplify presentation of algorithms.

**Definition 1 (sequences).** *A sequence of length  $n$ , say  $\bar{x} = \langle x_1, \dots, x_n \rangle$ , is an element of  $X^n$ . In particular, an element of  $\{0, 1\}^n$  is called a binary sequence. We say that a sequence  $\bar{x} \in X^n$  is sorted if  $x_i \geq x_{i+1}$ ,  $1 \leq i < n$ . Given two sequences  $\bar{x} = \langle x_1, \dots, x_n \rangle$  and  $\bar{y} = \langle y_1, \dots, y_m \rangle$  we define concatenation as  $\bar{x} :: \bar{y} = \langle x_1, \dots, x_n, y_1, \dots, y_m \rangle$ . We use also the following subsequence notation:*

$\bar{x}_{odd} = \langle x_1, x_3, \dots \rangle$ ,  $\bar{x}_{even} = \langle x_2, x_4, \dots \rangle$ ,  $\bar{x}_{a,\dots,b} = \langle x_a, \dots, x_b \rangle$ ,  $1 \leq a \leq b \leq n$ , and the prefix/suffix operators:  $\text{pref}(i, \bar{x}) = \bar{x}_{1,\dots,i}$  and  $\text{suff}(i, \bar{x}) = \bar{x}_{i,\dots,n}$ ,  $1 \leq i \leq n$ . The number of a given value  $b$  in  $\bar{x}$  is denoted by  $|\bar{x}|_b$  and the result of removing all occurrences of  $b$  in  $\bar{x}$  is written as  $\text{drop}(b, \bar{x})$ .

Let  $n, m \in \mathbb{N}$ . We define a domination relation  $\succeq$  on  $X^n \times X^m$ . Let  $\bar{x} \in X^n$  and  $\bar{y} \in X^m$ , then:  $\bar{x} \succeq \bar{y} \iff \forall_{i \in \{1,\dots,n\}} \forall_{j \in \{1,\dots,m\}} x_i \geq y_j$

**Definition 2 (zip operator).** For  $m \geq 1$  given sequences (column vectors)  $\bar{x}^i = \langle x_1^i, x_2^i, \dots, x_{n_i}^i \rangle$ ,  $1 \leq i \leq m$  and  $n_1 \geq n_2 \geq \dots \geq n_m$ , let us define the zip operation that outputs the elements of the vectors in row-major order:

$$\text{zip}(\bar{x}^1, \dots, \bar{x}^m) = \begin{cases} \bar{x}^1 & \text{if } m = 1 \\ \text{zip}(\bar{x}^1, \dots, \bar{x}^{m-1}) & \text{if } |\bar{x}^m| = 0 \\ \langle x_1^1, x_1^2, \dots, x_1^m \rangle :: \text{zip}(\bar{x}_{2,\dots,n_1}^1, \dots, \bar{x}_{2,\dots,n_m}^m) & \text{otherwise} \end{cases}$$

We construct and use comparator networks in this paper. The standard definitions and properties of them can be found, for example, in [13]. The only difference is that we assume that the output of any sorting operation or comparator is in a non-increasing order.

**Definition 3 (m-sorter).** A comparator network  $f^m$  is a sorting network (or m-sorter), if for each  $\bar{x} \in X^m$ ,  $f^m(\bar{x})$  is sorted.

In the pairwise sorting network, the first step is to split the input into two equally sized sequences  $\bar{x}$  and  $\bar{y}$ , such that for any  $i$ ,  $x_i \geq y_i$ . Then  $\bar{x}$  and  $\bar{y}$  are sorted independently and finally merged. Even after sorting, the property  $x_i \geq y_i$  is maintained (see [15]). For example, the pair of sequences  $\langle 110, 100 \rangle$  are pairwise sorted. We would like to extend this notion to cover larger number of sequences, let's say  $m \geq 2$ . For example, the tuple  $\langle 111, 110, 100, 000 \rangle$  is 4-wise (sorted). The following definition captures this idea.

**Definition 4 (m-wise sequences).** Let  $c, k, m \in \mathbb{N}$ ,  $1 \leq k$  and  $k/m \leq c$ . Moreover, let  $k_i = \min(c, \lfloor k/i \rfloor)$  and  $\bar{x}^i \in X^{k_i}$ ,  $1 \leq i \leq m$ . The tuple  $\langle \bar{x}^1, \dots, \bar{x}^m \rangle$  is  $m$ -wise of order  $(c, k)$  if:

1.  $\forall_{1 \leq i \leq m} \bar{x}^i$  is sorted,
2.  $\forall_{1 \leq i \leq m-1} \forall_{1 \leq j \leq n_{i+1}} x_j^i \geq x_j^{i+1}$ .

**Observation 1.** Let a tuple  $\langle \bar{x}^1, \dots, \bar{x}^m \rangle$  be  $m$ -wise of order  $(c, k)$ . Then:

1.  $|\bar{x}^1| \geq |\bar{x}^2| \geq \dots \geq |\bar{x}^m| = \lfloor k/m \rfloor$ ,
2.  $\sum_{i=1}^m |\bar{x}^i| \geq k$ ,
3. if  $|\bar{x}^{i-1}| > |\bar{x}^i| + 1$  then  $|\bar{x}^i| = \lfloor k/i \rfloor$ .

*Proof.* The first statement is obvious. To prove the second one let  $k_i = |\bar{x}^i|$ ,  $1 \leq i \leq m$ . Then, if  $k_i = c$  for each  $1 \leq i \leq m$ , we have  $\sum_{i=1}^m k_i = mc \geq mk/m = k$  and we are done. Let  $1 \leq i \leq m$  be the first index such that  $k_i \neq c$ , therefore  $k_i = \lfloor k/i \rfloor < c$ . Thus, for each  $1 \leq j < i$ :  $k_j = c > k_i$ , therefore  $k_j \geq k_i + 1$ . From this we get that  $\sum_{j=1}^m k_j \geq \sum_{j=1}^i k_j \geq i \lfloor k/i \rfloor + i - 1 \geq k$ .

The third one can be easily proved by contradiction. Assume that  $k_i = c$ , then from the first property  $k_{i-1} \geq k_i = c$ . Therefore,  $k_{i-1} = \min(c, \lfloor k/(i-1) \rfloor) \geq c$ , so  $k_{i-1} = c$ , a contradiction.  $\square$

**Definition 5 (top  $k$  sorted sequence).** A sequence  $\bar{x} \in X^n$  is top  $k$  sorted, with  $k \leq n$ , if  $\langle x_1, \dots, x_k \rangle$  is sorted and  $\langle x_1, \dots, x_k \rangle \succeq \langle x_{k+1}, \dots, x_n \rangle$ .

**Definition 6 (m-wise merger).** A comparator network  $f_{(c,k)}^s$  is a  $m$ -wise merger of order  $(c, k)$ , if for each  $m$ -wise tuple  $T = \langle \bar{x}^1, \dots, \bar{x}^m \rangle$  of order  $(c, k)$ , such that  $s = \sum_{i=1}^m |\bar{x}^i|$ ,  $f_{(c,k)}^s(T)$  is top  $k$  sorted.

**Definition 7 (m-odd-even merger).** A comparator network  $f_k^s$  is a  $m$ -odd-even merger of order  $k$ , if for each tuple  $T = \langle \bar{x}^1, \dots, \bar{x}^m \rangle$ , where each  $\bar{x}^i$  is top  $k$  sorted and  $s = \sum_{i=1}^m |\bar{x}^i|$ ,  $f_k^s(T)$  is top  $k$  sorted.

**Definition 8 (selection network).** A comparator network  $f_k^n$  (where  $k \leq n$ ) is a  $k$ -selection network, if for each  $\bar{x} \in X^n$ ,  $f_k^n(\bar{x})$  is top  $k$  sorted.

A clause is a disjunction of literals (Boolean variables  $x$  or their negation  $\neg x$ ). A CNF formula is a conjunction of one or more clauses. Cardinality constraints are of the form  $x_1 + \dots + x_n \sim k$ , where  $k \in \mathbb{N}$  and  $\sim$  belongs to  $\{<, \leq, =, \geq, >\}$ . We will focus on cardinality constraints with less-than relation, i.e.  $x_1 + \dots + x_n < k$ . The other can be easily translated to such form (see [3]).

In [1,3,9,10] authors are using sorting networks for an encoding of cardinality constraints, where inputs and outputs of a comparator are Boolean variables and comparators are encoded as a CNF formula. In addition, the  $k$ -th greatest output variable  $y_k$  of the network is forced to be 0 by adding  $\neg y_k$  as a clause to the formula that encodes  $x_1 + \dots + x_n < k$ . We use similar approach, but rather than using simple comparators (2-sorters), we also use comparators of higher order as building blocks. The  $m$ -sorter can be encoded as follows: for input variables  $\bar{x}$  and output variables  $\bar{y}$ , we add the set of clauses  $\{x_{i_1} \wedge \dots \wedge x_{i_p} \Rightarrow y_p : 1 \leq p \leq m, 1 \leq i_1 < \dots < i_p \leq m\}$ . Therefore, we need  $m$  auxiliary variables and  $2^m - 1$  clauses.

### 3 Generalized Selection Networks

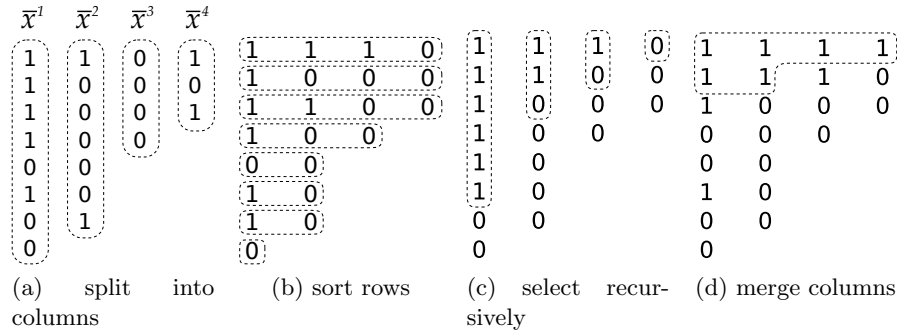
Here we present two novel constructions for selection networks which uses sorters of arbitrary size as components. We want to apply our algorithms for CNF encoding, therefore the only non-trivial operation that we are allowed to use in generalized comparator networks is  $sort^m : X^m \rightarrow X^m$ , which is a  $m$ -sorter. Here (and in the rest of the paper) we use it as a black box, but keep in mind that in the actual implementation one should encode the  $m$ -sorter using the standard procedure explained at the end of Section 2. We would also like to note that only first  $k$  output variables for each selection network is of interest, but to stay consistent with the definitions of Section 2, we write our algorithms so that the size of the output is the same as the size of the input. To this end we introduce the variable  $\overline{out}$  in which we store all throw-away variables in arbitrary order. The sequence  $\overline{out}$  is then appended to the output of the algorithms.

### 3.1 m-Wise Selection Network

We begin with the algorithm for constructing the  $m$ -Wise Selection Network (Network 1) and we prove that it is correct. In Network 1 we use  $mw\_merge_{(c,k)}^s$ , that is, a  $m$ -Wise Merger of order  $(c,k)$ , as a block box. We give detailed constructions of  $m$ -Wise Merger for  $m = 4$  in the next section.

The idea we use is the generalization of the one used in Pairwise Cardinality Network from [9] which is based on the Pairwise Sorting Network by Parberry [15]. First, we split the input sequence into  $m$  columns of non-increasing sizes (lines 2–5) and we sort rows using sorters (lines 6–8). Then we recursively run the selection algorithm on each column (lines 9–11), where at most  $\lfloor k/i \rfloor$  items are selected from the  $i$ -th column. In obtained outputs, selected items are sorted and form prefixes of the columns. The prefixes are padded with zeroes (with  $\perp$ 's) in order to get the input sizes required by the  $m$ -wise property (Definition 4) and, finally, they are passed to the merging procedure (line 12–13). The base case, when  $k = 1$ , is handled by the auxiliary network  $max^n$ , which outputs the maximum of  $n$  elements. The standard construction of  $max^n$  uses  $n - 1$  2-sorters.

*Example 1.* In Figure 1 we present a sample run of Network 1. The input is a sequence 1111010010000010000101, with parameters  $\langle n_1, n_2, n_3, n_4, k \rangle = \langle 8, 7, 4, 3, 6 \rangle$ . First step (Figure 1a) is to arrange the input in columns (lines 2–5). In this example we get  $\bar{x}^1 = \langle 11110100 \rangle$ ,  $\bar{x}^2 = \langle 1000001 \rangle$ ,  $\bar{x}^3 = \langle 0000 \rangle$  and  $\bar{x}^4 = \langle 101 \rangle$ . Next we sort rows using 1, 2, 3 or 4-sorters (lines 6–8), the result is visible in Figure 1b. We make recursive calls in lines 9–11 of the algorithm. Items selected recursively in this step are marked on Figure 1c. Notice that in  $i$ -th column we only need to select  $\lfloor k/i \rfloor$  largest elements. This is because of the initial sorting of the rows. Next comes the merging step, which is selecting  $k$  largest elements from the results of the previous step. How exactly those elements are obtained and outputted depends on the implementation. We choose the convention that the resulting  $k$  elements must be placed in the major-row order in our column representation of the input (see Figure 1d).



**Fig. 1.** Sample run of the 4-Wise Selection Network.

**Network 1**  $mw\_sel_k^n$ 


---

**Input:**  $\bar{x} \in X^n$ ;  $n_1, \dots, n_m \in \mathbb{N}$  where  $n > n_1 \geq \dots \geq n_m$  and  $\sum n_i = n$ ;  $1 \leq k \leq n$

- 1: **if**  $k = 1$  **then return**  $max^n(\bar{x})$
- 2:  $offset = 1$
- 3: **for all**  $i \in \{1, \dots, m\}$  **do** ▷ Splitting the input into columns.
- 4:    $\bar{x}^i \leftarrow \langle x_{offset}, \dots, x_{offset+n_i-1} \rangle$
- 5:    $offset += n_i$
- 6: **for all**  $i \in \{1, \dots, n_1\}$  **do** ▷ Sorting rows.
- 7:    $m' = \max\{j : n_j \geq i\}$
- 8:    $\bar{y}^i \leftarrow sort^{m'}(\langle x_i^1, \dots, x_i^{m'} \rangle)$
- 9: **for all**  $i \in \{1, \dots, m\}$  **do** ▷ Recursively selecting items in columns.
- 10:    $k_i = \min(n_1, \lfloor k/i \rfloor)$ ;  $l_i = \min(n_i, \lfloor k/i \rfloor)$  ▷  $k_i \geq l_i$
- 11:    $\bar{z}^i \leftarrow mw\_sel_{l_i}^{n_i}(\bar{y}_i^1, \dots, \bar{y}_i^{n_i})$
- 12:  $s = \sum_{i=1}^m k_i$ ;  $c = k_1$ ;  $\overline{out} = \text{suff}(l_1 + 1, \bar{z}^1) :: \dots :: \text{suff}(l_m + 1, \bar{z}^m)$
- 13:  $\overline{res} \leftarrow mw\_merge_{(c,k)}^s(\langle \text{pref}(l_1, \bar{z}^1) :: \perp^{k_1-l_1}, \dots, \text{pref}(l_m, \bar{z}^m) \rangle :: \perp^{k_m-l_m})$
- 14: **return**  $\text{drop}(\perp, \overline{res}) :: \overline{out}$

---

In the following we will prove the correctness of Network 1 using the well-known 0-1 Principle, that is, we will consider binary sequences only.

**Lemma 1.** Let  $\bar{t}^i = \langle \bar{y}_i^1, \dots, \bar{y}_i^{n_i} \rangle$ , where  $\bar{y}^j$ ,  $j = 1, \dots, n_1$ , is the result of Step 8 in Network 1. For each  $1 \leq i < m$ :  $|\bar{t}^i|_1 \geq |\bar{t}^{i+1}|_1$ .

*Proof.* Take any  $1 \leq i < m$ . Consider element  $y_i^j$  (for some  $1 \leq j \leq n_i$ ). Since  $\bar{y}^j$  is sorted, we have  $y_i^j \geq y_{i+1}^j$ , therefore if  $y_{i+1}^j = 1$  then  $y_i^j = 1$ . Thus  $|\bar{t}^i|_1 \geq |\bar{t}^{i+1}|_1$ .  $\square$

**Corollary 1.** For each  $1 \leq i \leq m$ , let  $\bar{z}^i$  be the result of the step 11 in Network 1. Then for each  $1 \leq i < m$ :  $|\bar{z}^i|_1 \geq |\bar{z}^{i+1}|_1$ .

*Proof.* For  $1 \leq i \leq m$ , let  $\bar{t}^i$  be the same as in Lemma 1. Take any  $1 \leq i < m$ . Comparator network only permute its input, therefore  $|\bar{z}^i|_1 = |mw\_sel_{s_i}^{n_i}(\bar{t}^i)|_1 = |\bar{t}^i|_1 \geq |\bar{t}^{i+1}|_1 = |mw\_sel_{s_{i+1}}^{n_{i+1}}(\bar{t}^{i+1})|_1 = |\bar{z}^{i+1}|_1$ . The inequality comes from Lemma 1.  $\square$

**Theorem 1.**  $mw\_sel_k^n$  is a  $k$ -selection network.

*Proof.* We prove by induction that for each  $n, k \in \mathbb{N}$  such that  $1 \leq k \leq n$  and each  $\bar{x} \in \{0, 1\}^n$ :  $mw\_sel_k^n(\bar{x})$  is top  $k$  sorted. If  $1 = k \leq n$  then  $mw\_sel_k^n = max^n$ , so the theorem is true. For the induction step assume that  $n \geq k \geq 2$ ,  $m \geq 2$  and for each  $(n^*, k^*) \prec (n, k)$  (in lexicographical order) the theorem holds. We have to prove the following two properties:

1. The tuple  $\langle \text{pref}(l_1, \bar{z}^1) :: \perp^{k_1-l_1}, \dots, \text{pref}(l_m, \bar{z}^m) :: \perp^{k_m-l_m} \rangle$  is  $m$ -wise of order  $(k_1, k)$ .
2. The sequence  $\bar{w} = \text{pref}(l_1, \bar{z}^1) :: \dots :: \text{pref}(l_m, \bar{z}^m)$  contains  $k$  largest elements from  $\bar{x}$ .

Ad. 1): Observe that for any  $i$ ,  $1 \leq i \leq m$ , we have  $n_i \leq n_1 < n$  and  $l_i \leq l_1 \leq k$ . Thus,  $(n_i, l_i) \prec (n, k)$  and  $\bar{z}_i$  is top  $l_i$  sorted due to the induction hypothesis. Therefore,  $\text{pref}(l_i, \bar{z}^i)$  is sorted and so is  $\text{pref}(l_i, \bar{z}^i) :: \perp^{k-l_i}$ . In this way, we prove that the first property of Definition 4 is satisfied. To prove the second one, fix  $1 \leq j \leq l_{i+1}$  and assume that  $z_j^{i+1} = 1$ . We are going to show that  $z_j^i = 1$ . Since  $\bar{z}^i$  and  $\bar{z}^{i+1}$  are both top  $l_{i+1}$  sorted (by the induction hypothesis) and since  $|\bar{z}^i|_1 \geq |\bar{z}^{i+1}|_1$  (from Corollary 1), we have  $|\text{pref}(l_{i+1}, \bar{z}^i)|_1 \geq |\text{pref}(l_{i+1}, \bar{z}^{i+1})|_1$ , so  $z_j^i = 1$ .

Ad. 2): It is easy to observe that  $\bar{z} = \bar{z}^1 :: \dots :: \bar{z}^m$  is a permutation of the input sequence  $\bar{x}$ . If all 1's in  $\bar{z}$  are in  $\bar{w}$ , we are done. So assume that there exists  $z_j^i = 1$  for some  $1 \leq i \leq m$ ,  $l_i < j \leq n_i$ . We will show that  $|\bar{w}|_1 \geq k$ . From the induction hypothesis we get  $\text{pref}(l_i, z^i) \succeq \langle z_j^i \rangle$ , which implies that  $|\text{pref}(l_i, z^i)|_1 = l_i$ . From (1) and the second property of Definition 4 it is clear that all  $z_t^s$  are 1's, where  $1 \leq s \leq i$  and  $1 \leq t \leq l_i$ , therefore  $|\text{pref}(l_i, \bar{z}^1) :: \dots :: \text{pref}(l_i, \bar{z}^i)|_1 = i \cdot l_i$ . Moreover, since  $j > l_i$ , we have  $l_i = \lfloor k/i \rfloor$ ; otherwise we would have  $j > n_i$ . If  $i = 1$ , then  $|\bar{w}|_1 \geq 1 \cdot l_1 = k$  and (2) holds.

Otherwise,  $l_1 > l_i$ , so from the definition of  $l_i$ ,  $l_1 \geq \dots \geq l_i$ , hence there exists  $r \geq 1$  such that  $\forall_{r < i' \leq i} l_r > l_{i'} = l_i$ . Notice that since  $|\text{pref}(l_i, z^i)|_1 = l_i$  and  $z_j^i = 1$  where  $j > l_i$  we get  $|z^i|_1 \geq l_i + 1$ . From Corollary 1 we have that for  $1 \leq r' \leq r$ :  $|\bar{z}^{r'}|_1 \geq l_i + 1$ . Using  $l_{r'} \geq l_r > l_i$  and the induction hypothesis we get that each  $\bar{z}^{r'}$  is top  $l_i + 1$  sorted, therefore  $|\text{pref}(l_i + 1, \bar{z}^{r'})|_1 = l_i + 1$ . We finally have that  $|\bar{w}|_1 \geq |\text{pref}(l_i + 1, \bar{z}^1) :: \dots :: \text{pref}(l_i + 1, \bar{z}^r)|_1 = r(l_i + 1) + (i - r)l_i = r(l_{r+1} + 1) + (i - r)l_{r+1} = i \cdot l_{r+1} + r \geq (r + 1) \lfloor k/(r + 1) \rfloor + r \geq k$ . In the second to last inequality, we use the facts:  $l_{r+1} = l_i = \lfloor k/i \rfloor < n_i \leq n_{r+1}$  from which  $l_{r+1} = \lfloor k/(r + 1) \rfloor$  follows.

From the statements (1) and (2) we can conclude that  $\text{mw\_merge}_{(n,k)}^s$  will return the  $k$  largest elements from  $\bar{x}$ , which completes the proof.  $\square$

### 3.2 m-Odd-Even Selection Network

Next we present the algorithm for constructing the  $m$ -Odd-Even Selection Network (Network 2) and we prove that it is correct. In Network 2 we use  $\text{oe\_merge}_k^s$  as a black box. It is a  $m$ -Odd-Even Merger of order  $k$ . We give detailed constructions of  $m$ -Odd-Even Merger for  $m = 4$  in the next section.

The idea we use is the generalization of the one used in Odd-Even Selection Network from [9] which is based on the Odd-Even Sorting Network by Batcher [6]. We arrange the input sequence into  $m$  columns of non-increasing sizes and we recursively run the selection algorithm on each column (lines 3–6), where at most  $k$  items are selected from each column. Notice that each column is represented by ranges derived from the increasing value of variable *offset*. Selected items are sorted and form prefixes of the columns and they are the input to the merging procedure (line 7–8).

*Example 2.* Assuming the same input sequence and parameters as in Example 1, the sample run of 4-Odd-Even Selection Network would be very similar to the



one presented in Figure 1, except we would not do the row sorting step, and in consequence we would need to recursively select  $k$  largest elements from each column.

---

**Network 2**  $oe\_sel_k^n$ 


---

**Input:**  $\bar{x} \in \{0, 1\}^n$ ;  $n_1, \dots, n_m \in \mathbb{N}$  where  $n > n_1 \geq \dots \geq n_m$  and  $\sum n_i = n$ ;  
 $1 \leq k \leq n$   
 1: **if**  $k = 1$  **then return**  $max^n(\bar{x})$   
 2:  $offset = 1$   
 3: **for all**  $i \in \{1, \dots, m\}$  **do**  
 4:      $k_i = \min(k, n_i)$   
 5:      $\bar{y}^i \leftarrow oe\_sel_{k_i}^{n_i}(\langle x_{offset}, \dots, x_{offset+n_i-1} \rangle)$   
 6:      $offset += n_i$   
 7:  $s = \sum_{i=1}^m k_i$ ;  $\overline{out} = \text{suff}(k_1 + 1, \bar{y}^1) :: \dots :: \text{suff}(k_m + 1, \bar{y}^m)$   
 8: **return**  $oe\_merge_k^s(\langle \text{pref}(k_1, \bar{y}^1), \dots, \text{pref}(k_m, \bar{y}^m) \rangle) :: \overline{out}$

---

**Theorem 2.**  $oe\_sel_k^n$  is a  $k$ -selection network.

*Proof.* It is easy to observe that  $\bar{y} = \bar{y}^1 :: \dots :: \bar{y}^m$  is a permutation of the input sequence  $\bar{x}$ . We prove by induction that for each  $n, k \in \mathbb{N}$  such that  $1 \leq k \leq n$  and each  $\bar{x} \in \{0, 1\}^n$ :  $oe\_sel_k^n(\bar{x})$  is top  $k$  sorted. If  $1 = k \leq n$  then  $oe\_sel_k^n = max^n$ , so the theorem is true. For the induction step assume that  $n \geq k \geq 2$ ,  $m \geq 2$  and for each  $(n^*, k^*) \prec (n, k)$  (in lexicographical order) the theorem holds. We have to prove that the sequence  $\bar{w} = \text{pref}(k_1, \bar{y}^1) :: \dots :: \text{pref}(k_m, \bar{y}^m)$  contains  $k$  largest elements from  $\bar{x}$ . If all 1's in  $\bar{y}$  are in  $\bar{w}$ , we are done. So assume that there exists  $y_j^i = 1$  for some  $1 \leq i \leq m$ ,  $k_i < j \leq n_i$ . We will show that  $|\bar{w}|_1 \geq k$ . Notice that  $k_i = k$ , otherwise  $j > k_i = n_i$  – a contradiction. Since  $|\bar{y}^i| = n_i \leq n_1 < n$ , from the induction hypothesis we get that  $\bar{y}^i$  is top  $k_i$  sorted. In consequence,  $\text{pref}(k_i, \bar{y}^i) \succeq \langle y_j^i \rangle$ , which implies that  $|\text{pref}(k_i, \bar{y}^i)|_1 = k_i = k$ . We conclude that  $|\bar{w}|_1 \geq |\text{pref}(k_i, \bar{y}^i)|_1 = k$ . Note also that in the case  $n = k$  we have all  $k_i = \min(n_i, k) < k$ , so the case is correctly reduced.

Finally, using  $oe\_merge_k^s$  the algorithm returns  $k$  largest elements from  $\bar{x}$ , which completes the proof.  $\square$

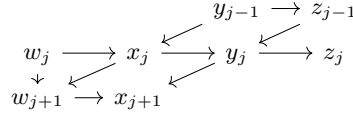
## 4 Merging Networks

In this section we give the detailed constructions of the networks  $4mw\_merge$  and  $4oe\_merge$  that merge four sequences (columns) obtained from the recursive calls in Networks 1 and 2. In the first construction we can assume that input columns form a tuple that is 4-wise, because rows were sorted before selecting top elements in each column. In the second one input columns are just top  $k$  sorted and rows are sorted in the final steps of the merging process. In the subsections 4.1 and 4.2 we present the 4-Wise Merger and 4-Column Odd-Even Merger, respectively.

#### 4.1 4-Wise Merging Networks

In this subsection the first merging algorithm for four columns is presented. The input to the merging procedure is  $R = \langle \text{pref}(n_1, \bar{y}^1), \dots, \text{pref}(n_m, \bar{y}^m) \rangle$ , where each  $\bar{y}^i$  is the output of the recursive call in Network 1. The main observation is the following: since  $R$  is  $m$ -wise, if you take each sequence  $\text{pref}(n_i, \bar{y}^i)$  and place them side by side, in columns, from left to right, then the sequences will be sorted in rows and columns. The goal of the networks is to put the  $k$  largest elements in top rows. It is done by sorting slope lines with decreasing slope rate, in lines 1–14 (similar idea can be found in [11]). The algorithm is presented in Network 3. The pseudo-code looks non-trivial, but it is because we need a separate sub-case every time we need to use either  $\text{sort}^2$ ,  $\text{sort}^3$  or  $\text{sort}^4$  operation, and this depends on the sizes of columns and the current slope.

After slope-sorting phase some elements might not be in the desired row-major order, therefore the correction phase is needed, which is the goal of the sorting operations in lines 15–18. Figure 2 shows the order relations of elements after  $i = \lceil \log n_1 \rceil$  iterations of the **while** loop (disregarding the upper index  $i$ , for clarity). Observe that the order should be possibly corrected between  $z_{j-1}$  and  $w_{j+1}$  and then the 4-tuples  $\langle x_j, w_j, z_{j-1}, y_{j-1} \rangle$  and  $\langle x_{j+1}, w_{j+1}, z_j, y_j \rangle$  should be sorted to get the row-major order. Lines 17–18 addresses certain corner cases of the correction phase.



**Fig. 2.** The order relation among elements of neighbouring rows. Arrows shows non-increasing order. Relations that follow from transitivity are not shown.

An input to Network 3 must be 4-wise of order  $(c, k)$  and in the output should be top  $k$  sorted. We prove it using the 0-1 principle, that is, in this subsection we assume that sequences (in particular, inputs) are binary.

Thus, the algorithm gets as input four sorted 0-1 columns with the additional property that the numbers of 1's in successive columns do not increase. Nevertheless, the differences between them can be quite big. The goal of each iteration of the main loop in Network 3 is to decrease the maximal possible difference by the factor of two. Therefore, after the main loop, the differences are bounded by one.

*Example 3.* A sample run of slope sorting phase of Network 3 is presented in Figure 3. The arrows represent the sorting order. Notice how the 1s are being *pushed* towards upper-right side. In the end, the differences between the number of 1s in consecutive columns are bounded by one.

In the  $i$ -th iteration of the loop the values of columns  $\bar{w}^i$ ,  $\bar{x}^i$ ,  $\bar{y}^i$  and  $\bar{z}^i$  are obtained by sorting the results of the previous iteration in slope lines with decreasing slope rate. The sizes of the sorted prefix of the columns can also

**Network 3**  $4w\_merge_{(c,k)}^s$ 


---

**Input:** 4-wise tuple  $\langle \bar{w}, \bar{x}, \bar{y}, \bar{z} \rangle$  of order  $(c, k)$ , where  $s = |\bar{w}| + |\bar{x}| + |\bar{y}| + |\bar{z}|$  and  $c = |\bar{w}|$ .

- 1:  $k_1 = |\bar{w}|$ ;  $k_2 = |\bar{x}|$ ;  $k_3 = |\bar{y}|$ ;  $k_4 = |\bar{z}|$
- 2:  $d \leftarrow \min\{l \in \mathbb{N} \mid 2^l \geq k_1\}$
- 3:  $h \leftarrow 2^d$ ;  $i \leftarrow 0$ ;  $\langle \bar{w}^0, \bar{x}^0, \bar{y}^0, \bar{z}^0 \rangle = \langle \bar{w}, \bar{x}, \bar{y}, \bar{z} \rangle$ ;  $h_0 \leftarrow h$
- 4: **while**  $h_i > 1$  **do** ▷ Define the  $(i+1)$ -th stage of  $4w\_merge_{(n,k)}^s$ .
- 5:    $i \leftarrow i + 1$ ;  $h_i \leftarrow h_{i-1}/2$
- 6:    $\langle \bar{w}^i, \bar{x}^i, \bar{y}^i, \bar{z}^i \rangle = \langle \bar{w}^{i-1}, \bar{x}^{i-1}, \bar{y}^{i-1}, \bar{z}^{i-1} \rangle$
- 7:   **for all**  $j \in \{1, \dots, \min(k_3 - h_i, k_4)\}$  **do**
- 8:     **if**  $j + 3h_i \leq k_1$  **and**  $j + 2h_i \leq k_2$  **then**  $sort^4(z_j^i, y_{j+h_i}^i, x_{j+2h_i}^i, w_{j+3h_i}^i)$
- 9:     **else if**  $j + 2h_i \leq k_2$  **then**  $sort^3(z_j^i, y_{j+h_i}^i, x_{j+2h_i}^i)$  ▷  $w_{j+3h_i}^i$  is not defined.
- 10:    **else**  $sort^2(z_j^i, y_{j+h_i}^i)$  ▷ Both  $x_{j+2h_i}^i$  and  $w_{j+3h_i}^i$  are not defined.
- 11:   **for all**  $j \in \{1, \dots, \min(k_2 - h_i, k_3, h_i)\}$  **do**
- 12:     **if**  $j + 2h_i \leq k_1$  **then**  $sort^3(y_j^i, x_{j+h_i}^i, w_{j+2h_i}^i)$
- 13:     **else**  $sort^2(y_j^i, x_{j+h_i}^i)$  ▷  $w_{j+2h_i}^i$  is not defined.
- 14:   **for all**  $j \in \{1, \dots, \min(k_1 - h_i, k_2, h_i)\}$  **do**  $sort^2(x_j^i, w_{j+h_i}^i)$   
▷ Define two more stages to correct local disorders.
- 15: **for all**  $j \in \{1, \dots, \min(k_1 - 2, k_4)\}$  **do**  $sort^2(z_j^i, w_{j+2}^i)$
- 16: **for all**  $j \in \{1, \dots, \min(k_2 - 1, k_4)\}$  **do**  $sort^4(y_j^i, z_j^i, w_{j+1}^i, x_{j+1}^i)$
- 17: **if**  $k_1 > k_4$  **and**  $k_2 = k_4$  **then**  $sort^3(y_{k_4}^i, z_{k_4}^i, w_{k_4+1}^i)$  ▷  $x_{k_4+1}^i$  is not defined.
- 18: **if**  $k \bmod 4 = 3$  **and**  $k_1 > k_3$  **then**  $sort^2(y_{k_4+1}^i, w_{k_4+2}^i)$  ▷  $y_{k_4+1}^i$  must be corrected.
- 19: **return**  $zip(\bar{w}^i, \bar{x}^i, \bar{y}^i, \bar{z}^i)$  ▷ Returns the columns in row-major order.

---

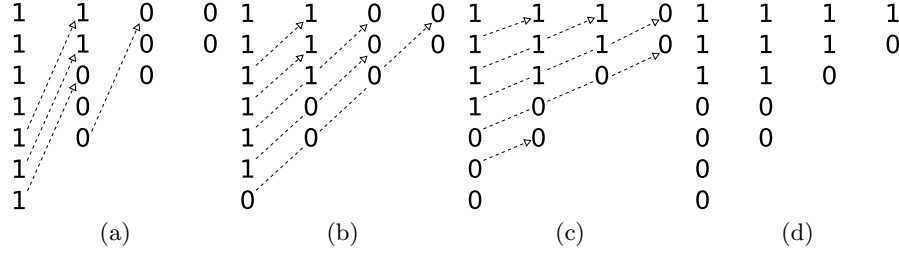
decrease in each iteration, but we would like to keep the  $k$  largest input elements in that prefixes. In the following observation and lemma we define and formulate the basic properties of the column lengths after each iteration.

**Observation 2.** Let  $k_1, \dots, k_4$  be as defined in Network 3. For each  $i$ ,  $0 \leq i \leq \lceil \log(k_1) \rceil$ , let  $c_i = \min(k_3, \lfloor k/4 \rfloor + h_i)$ ,  $b_i = \min(k_2, c_i + h_i)$  and  $a_i = \min(k_1, b_i + h_i)$ . Then we have:  $k_1 \geq a_i \geq b_i \geq c_i \geq \lfloor k/4 \rfloor$  and the inequalities:  $a_i - b_i \leq h_i$ ,  $b_i - c_i \leq h_i$  and  $c_i - \lfloor k/4 \rfloor \leq h_i$  are true.

*Proof.* From Observation 1.(1) we have  $k_1 \geq k_2 \geq k_3 \geq \lfloor k/4 \rfloor$ . It follows that  $c_i \geq \lfloor k/4 \rfloor$  and  $b_i \geq \min(k_3, \lfloor k/4 \rfloor + h_i) = c_i$  and  $k_1 \geq a_i \geq \min(k_2, c_i + h_i) = b_i$ . Moreover, one can see that  $c_i - \lfloor k/4 \rfloor = \min(k_3 - \lfloor k/4 \rfloor, h_i) \leq h_i$ ,  $b_i - c_i = \min(k_2 - c_i, h_i) \leq h_i$  and  $a_i - b_i = \min(k_1 - b_i, h_i) \leq h_i$ , so we are done.  $\square$

**Lemma 2.** Let  $a_i, b_i, c_i$ ,  $0 \leq i \leq \lceil \log(k_1) \rceil$ , be as defined in Observation 2. Let  $\tilde{w}^i = \text{pref}(a_i, \bar{w}^i)$ ,  $\tilde{x}^i = \text{pref}(b_i, \bar{x}^i)$ ,  $\tilde{y}^i = \text{pref}(c_i, \bar{y}^i)$  and  $\tilde{z}^i = \bar{z}^i$ . Then only the items in  $\tilde{w}^i$ ,  $\tilde{x}^i$ ,  $\tilde{y}^i$  and  $\tilde{z}^i$  take part in the  $i$ -th iteration of sorting operations in lines 8-14 of Network 3.

*Proof.* An element of the vector  $\bar{z}^i$ , that is,  $z_j^i$  is sorted in one of the lines 8–10 of Network 3, thus for all such  $j$  that  $1 \leq j \leq k_4 = \lfloor k/4 \rfloor$ . An element  $y_j^i$  of  $\bar{y}^i$  is sorted in lines 8–10 of the first inner loop and in lines 12–13 of the second inner loop. In the first three of those lines we have the bounds on



**Fig. 3.** Sample run of the slope-sorting phase of 4-Wise Merging Network.

$j$ :  $1 + h_i \leq j \leq \min(k_3, k_4 + h_i)$  and in the last three lines - the bounds:  $1 \leq j \leq \min(k_3, h_i)$ . The sum of these two intervals is  $1 \leq j \leq \min(k_3, \lfloor k/4 \rfloor + h_i) = c_i$ . Similarly, we can analyse the operations on  $x_j^i$  in lines 8–10, 12–13 and 14. The range of  $j$  is the sum of the following disjoint three intervals:  $[1 + 2h_i, \min(k_2, k_3 + h_i, k_4 + 2h_i)]$ ,  $[1 + h_i, \min(k_3 + h_i, 2h_i)]$  and  $[1, \min(k_2, h_i)]$  that give us the interval  $[1, \min(k_2, k_3 + h_i, k_4 + 2h_i)] = [1, b_i]$  as their sum. The analysis of the range of  $j$  used in the operations on  $w_j^i$  in Network 3 can be done in the same way.  $\square$

The next lemma formulates the key invariants of the main loop in Network 3. They will be used in the proof of the main theorem in this section stating the merging properties of the network.

**Lemma 3.** *Let  $\tilde{w}^i$ ,  $\tilde{x}^i$ ,  $\tilde{y}^i$  and  $\tilde{z}^i$  be as defined in Lemma 2. Then for all  $i$ ,  $0 \leq i \leq \lceil \log_2 k_1 \rceil$ , after the  $i$ -th iteration of the while loop in Network 3 the sequences  $\tilde{w}^i, \tilde{x}^i, \tilde{y}^i, \tilde{z}^i$  are of the form  $1^{p_i}0^*$ ,  $1^{q_i}0^*$ ,  $1^{r_i}0^*$  and  $1^{s_i}0^*$ , respectively, and:*

$$p_i \geq q_i \geq r_i \geq s_i, \quad (1)$$

$$p_i - q_i \leq h_i \text{ and } q_i - r_i \leq h_i \text{ and } r_i - s_i \leq h_i, \quad (2)$$

$$p_i + q_i + r_i + s_i \geq \min(k, p_0 + q_0 + r_0 + s_0). \quad (3)$$

*Proof.* By induction. At the beginning we have  $h_0 \geq k_1 \geq k_2 \geq k_3 \geq k_4 = \lfloor k/4 \rfloor$  and therefore  $\tilde{w}^0 = \bar{w}$ ,  $\tilde{x}^0 = \bar{x}$ ,  $\tilde{y}^0 = \bar{y}$  and  $\tilde{z}^0 = \bar{z}$ . All four sequences  $\bar{w}, \bar{x}, \bar{y}, \bar{z}$  are sorted (by Definition 4), thus, they are of the form  $1^{p_0}0^*$ ,  $1^{q_0}0^*$ ,  $1^{r_0}0^*$ , and  $1^{s_0}0^*$  respectively. By Definition 4.(2), for each pair of sequences:  $(\bar{w}_{1..k_2}, \bar{x})$ ,  $(\bar{x}_{1..k_3}, \bar{y})$  and  $(\bar{y}_{1..k_4}, \bar{z})$ , if there is a 1 on the  $j$  position in the right sequence, it must be a corresponding 1 on the same position in the left one. Therefore, we have:  $p_0 \geq q_0 \geq r_0 \geq s_0 \geq 0$ . Moreover,  $p_0 - q_0 \leq p_0 \leq k_1 \leq h_0$ ,  $q_0 - r_0 \leq q_0 \leq k_2 \leq h_0$  and  $r_0 - s_0 \leq r_0 \leq k_3 \leq h_0$ . Finally,  $p_0 + q_0 + r_0 + s_0 \geq \min(k, p_0 + q_0 + r_0 + s_0)$ , thus the lemma holds for  $i = 0$ .

In the inductive step  $i > 0$  observe that the elements of  $\tilde{w}^i$ ,  $\tilde{x}^i$ ,  $\tilde{y}^i$  and  $\tilde{z}^i$  are defined by the sort operations over the elements with the same indices from vectors  $\tilde{w}^{i-1}$ ,  $\tilde{x}^{i-1}$ ,  $\tilde{y}^{i-1}$  and  $\tilde{z}^{i-1}$ . This means that the values of  $w_{a_i+1, \dots, a_{i+1}}^{i-1}$ ,

$x_{b_i+1, \dots, b_{i+1}}^{i-1}$  and  $y_{c_i+1, \dots, c_{i+1}}^{i-1}$  are not used in the  $i$ -th iteration. Therefore, the numbers of 1's in columns that are sorted in the  $i$ -th iteration are defined by values:  $p'_{i-1} = \min(a_i, p_{i-1})$ ,  $q'_{i-1} = \min(b_i, q_{i-1})$ ,  $r'_{i-1} = \min(c_i, r_{i-1})$  and  $s'_{i-1} = s_{i-1}$ . In the following we will prove that the numbers with primes have the same properties as those without them.

$$p'_{i-1} \geq q'_{i-1} \geq r'_{i-1} \geq s'_{i-1}, \quad (4)$$

$$p'_{i-1} - q'_{i-1} \leq h_{i-1} \text{ and } q'_{i-1} - r'_{i-1} \leq h_{i-1} \text{ and } r'_{i-1} - s'_{i-1} \leq h_{i-1}, \quad (5)$$

$$p'_{i-1} + q'_{i-1} + r'_{i-1} + s'_{i-1} \geq \min(k, p_{i-1} + q_{i-1} + r_{i-1} + s_{i-1}). \quad (6)$$

The proofs of inequalities in Eq. 4 are quite direct and follow from the monotonicity of  $\min$ . For example, we can observe that  $p'_{i-1} = \min(a_i, p_{i-1}) \geq \min(b_i, q_{i-1}) = q'_{i-1}$ , since we have  $a_i \geq b_i$  and  $p_{i-1} \geq q_{i-1}$ , by Observation 2 and the induction hypothesis. The others can be shown in the same way.

Let us now prove one of the inequalities of Eq. (5), say, the second one. We have  $q'_{i-1} - r'_{i-1} = \min(b_i, q_{i-1}) - \min(c_i, r_{i-1}) \leq \min(c_i + h_i, r_{i-1} + h_{i-1}) - \min(c_i, r_{i-1}) \leq h_{i-1}$ , by Observation 2, the fact that  $h_{i-1} = 2h_i$  and the induction hypothesis. The proofs of the others are similar.

The proof of Eq. (6) is only needed if at least one of the following inequalities are true:  $p'_{i-1} < p_{i-1}$ ,  $q'_{i-1} < q_{i-1}$  or  $r'_{i-1} < r_{i-1}$ . Obviously, the inequalities are equivalent to  $a_i < p_{i-1}$ ,  $b_i < q_{i-1}$  and  $c_i < r_{i-1}$ , respectively. Therefore, to prove Eq. 6 we consider now three separate cases: (1)  $a_i \geq p_{i-1}$  and  $b_i \geq q_{i-1}$  and  $c_i < r_{i-1}$ , (2)  $a_i \geq p_{i-1}$  and  $b_i < q_{i-1}$  and (3)  $a_i < p_{i-1}$ .

In the case (1) we have  $p'_{i-1} = p_{i-1}$ ,  $q'_{i-1} = q_{i-1}$  and  $r'_{i-1} = c_i = \min(k_3, h_i + \lfloor k/4 \rfloor) < r_{i-1} \leq q_{i-1} \leq p_{i-1}$ . It follows that  $p'_{i-1} + q'_{i-1} + r'_{i-1} = p_{i-1} + q_{i-1} + c_i \geq c_i + 1 + c_i + 1 + c_i = 3c_i + 2$ . Since  $k_3 \geq r_{i-1} \geq c_i + 1 = \min(k_3, \lfloor k/4 \rfloor + h_i) + 1$ , we can observe that  $c_i$  must be equal to  $\lfloor k/4 \rfloor + h_i$ . In addition, by the induction hypothesis we have  $s_{i-1} \geq r_{i-1} - h_{i-1} \geq c_i + 1 - 2h_i$ . Merging those facts we can conclude that  $p'_{i-1} + q'_{i-1} + r'_{i-1} + s'_{i-1} \geq 4c_i + 3 - 2h_i = 4 \lfloor k/4 \rfloor + 4h_i + 3 - 2h_i \geq k$ , so we are done in this case.

In the case (2) we have  $p'_{i-1} = p_{i-1}$  and  $q'_{i-1} = b_i = \min(k_2, c_i + h_i) < q_{i-1} \leq p_{i-1}$ . It follows that  $p'_{i-1} + q'_{i-1} \geq 2b_i + 1$ . Since  $k_2 \geq q_{i-1} \geq b_i + 1 = \min(k_2, c_i + h_i) + 1$ , we can observe that  $b_i$  must be equal to  $c_i + h_i$ . In addition, by the induction hypothesis and Observation 2, we can bound  $r'_{i-1}$  as  $r'_{i-1} = \min(c_i, r_{i-1}) \geq \min(b_i - h_i, q_{i-1} - h_{i-1}) \geq b_i + 1 - 2h_i$ . Therefore,  $p'_{i-1} + q'_{i-1} + r'_{i-1} \geq 3b_i + 2 - 2h_i = 3c_i + 2 + h_i$ . Since  $c_i$  is defined as  $\min(k_3, \lfloor k/4 \rfloor + h_i)$ , we have to consider two subcases of the possible value of  $c_i$ . If  $c_i = k_3 \leq \lfloor k/4 \rfloor + h_i$ , then we have  $k_2 \geq q_{i-1} \geq b_i + 1 = c_i + h_i + 1 \geq k_3 + 2$ . By Observation 1.(3),  $k_3$  must be equal to  $\lfloor k/3 \rfloor$ , thus  $3c_i + 2 = 3k_3 + 2 \geq k$ , and we are done. Otherwise, we have  $c_i = \lfloor k/4 \rfloor + h_i$  and since  $s'_{i-1} = s_{i-1} \geq r_{i-1} - h_{i-1} \geq b_i + 1 - 4h_i = c_i + 1 - 3h_i$ , we can conclude that  $p'_{i-1} + q'_{i-1} + r'_{i-1} + s'_{i-1} \geq 4c_i + 3 - 2h_i = 4 \lfloor k/4 \rfloor + 3 + 2h_i \geq k$ .

The last case  $a_i < p_{i-1}$  can be proved by the similar arguments. Having Eqs. (4,5,6), we can start proving the inequalities from the lemma. Observe that in Network 4 the values of vectors  $\bar{w}^i$ ,  $\bar{x}^i$ ,  $\bar{y}^i$  and  $\bar{z}^i$  are defined with the help of three types of sorters:  $sort^4$ ,  $sort^3$  and  $sort^2$ . The smaller sorters are used, when the corresponding index is out of the range and an input item is

not available. In the following analysis we would like to deal only with  $sort^4$  and in the case of smaller sorters we extend artificially their inputs and outputs with 1's at the left end and 0's at the right end. For example, in line 18 we have  $\langle y_j^i, x_{j+h_i}^i \rangle \leftarrow sort^2(y_j^{i-1}, x_{j+h_i}^{i-1})$  and we can analyse this operation as  $\langle 1, y_j^i, x_{j+h_i}^i, 0 \rangle \leftarrow sort^4(1, y_j^{i-1}, x_{j+h_i}^{i-1}, 0)$ . The 0 input corresponds to the element of  $\bar{w}^{i-1}$  with index  $j + 2h_i$ , where  $j + 2h_i > k_1 \geq a_i$ , and the 1 input corresponds to the element of  $\bar{z}^{i-1}$  with index  $j - h_i$ , where  $j - h_i < 0$ . A similar situation is in lines 10, 12, 16 and 22, where  $sort^2$  and  $sort^3$  are used. Therefore, in the following we assume that elements of input sequences  $\bar{w}^{i-1}$ ,  $\bar{x}^{i-1}$ ,  $\bar{y}^{i-1}$  and  $\bar{z}^{i-1}$  with negative indices are equal to 1 and elements of the inputs with indices above  $a_i$ ,  $b_i$ ,  $c_i$  and  $\lfloor k/4 \rfloor$ , respectively, are equal to 0. This assumption does not break the monotonicity of the sequences and we also have the property that  $w_j^{i-1} = 1$  if and only if  $j \leq p'_{j-1}$  (and similar ones for  $\bar{x}^{i-1}$  and  $q'_{i-1}$ , and so on).

It should be clear now that, under the assumption above, we have:

$$w_j^i = \min(w_j^{i-1}, x_{j-h_i}^{i-1}, y_{j-2h_i}^{i-1}, z_{j-3h_i}^{i-1}) \quad \text{for } 1 \leq j \leq a_i, \quad (7a)$$

$$x_j^i = 2nd(w_{j+h_i}^{i-1}, x_j^{i-1}, y_{j-h_i}^{i-1}, z_{j-2h_i}^{i-1}) \quad \text{for } 1 \leq j \leq b_i, \quad (7b)$$

$$y_j^i = 3rd(w_{j+2h_i}^{i-1}, x_{j+h_i}^{i-1}, y_j^{i-1}, z_{j-h_i}^{i-1}) \quad \text{for } 1 \leq j \leq c_i, \quad (7c)$$

$$z_j^i = \max(w_{j+3h_i}^{i-1}, x_{j+2h_i}^{i-1}, y_{j+h_i}^{i-1}, z_j^{i-1}) \quad \text{for } 1 \leq j \leq \lfloor k/4 \rfloor, \quad (7d)$$

where 2nd and 3rd denote the second and the third smallest element of its input, respectively. Since the functions min, 2nd, 3rd and max are monotone and the input sequences are monotone, we can conclude that  $w_j^i \geq w_{j+1}^i$ ,  $x_j^i \geq x_{j+1}^i$ ,  $y_j^i \geq y_{j+1}^i$  and  $z_j^i \geq z_{j+1}^i$ . Let  $p_i$ ,  $q_i$ ,  $r_i$  and  $s_i$  denote the numbers of 1's in them. Clearly, we have  $p_i + q_i + r_i + s_i = p'_{i-1} + q'_{i-1} + r'_{i-1} + s'_{i-1}$ , thus  $p_i + q_i + r_i + s_i \geq \min(k, p_{i-1} + q_{i-1} + r_{i-1} + s_{i-1}) \geq \min(k, p_0 + q_0 + r_0 + s_0)$ , by the induction hypothesis. Thus, we have proved monotonicity of  $\bar{w}^i$ ,  $\bar{x}^i$ ,  $\bar{y}^i$  and  $\bar{z}^i$  and that Eq. (3) holds.

To prove Eq. (2) we would like to show that  $p_i - h_i \leq q_i$ ,  $q_i - h_i \leq r_i$ ,  $r_i - h_i \leq s_i$ , that is, that the following equalities are true:  $x_{p_i-h_i}^i = 1$ ,  $y_{q_i-h_i}^i = 1$  and  $z_{r_i-h_i}^i = 1$ . The first equality follows from the fact that  $w_{p_i}^i = 1$  and  $w_{p_i}^i \leq x_{p_i-h_i}^i$ , because they are output in this order by a single sort operation. The other two equalities can be shown by the similar arguments.

The last equation we have to prove is (1). By the induction hypothesis and our assumption we have  $w_j^{i-1} \geq x_j^{i-1} \geq y_j^{i-1} \geq z_j^{i-1}$ , for any  $j$ . We know also that the vectors are non-increasing. We use these facts to show that  $w_{q_i}^i = 1$ , which is equivalent to  $p_i \geq q_i$ . Since  $w_{q_i}^i = \min(w_{q_i}^{i-1}, x_{q_i-h_i}^{i-1}, y_{q_i-2h_i}^{i-1}, z_{q_i-3h_i}^{i-1})$ , we have to prove that all the arguments of the min function are 1's. From the definition of  $q_i$  we have  $1 = x_{q_i}^i = 2nd(w_{q_i+h_i}^{i-1}, x_{q_i}^{i-1}, y_{q_i-h_i}^{i-1}, z_{q_i-2h_i}^{i-1})$ , thus the maximum of any pair of arguments of 2nd must be 1. Now we can see that  $w_{q_i}^{i-1} \geq \max(w_{q_i+h_i}^{i-1}, x_{q_i}^{i-1}) \geq 1$ ,  $x_{q_i-h_i}^{i-1} \geq \max(x_{q_i}^{i-1}, y_{q_i-h_i}^{i-1}) \geq 1$ ,  $y_{q_i-2h_i}^{i-1} \geq \max(y_{q_i-h_i}^{i-1}, z_{q_i-2h_i}^{i-1}) \geq 1$  and  $z_{q_i-3h_i}^{i-1} \geq \max(y_{q_i-h_i}^{i-1}, z_{q_i-2h_i}^{i-1}) \geq 1$ . In the last inequality we use the fact that for any  $j$  it is true that  $z_{j-2h_i}^{i-1} \geq y_j^{i-1}$  (because

$r'_{i-1} - 2h_i \leq s'_{i-1}$ , by Eq. (5)). Thus,  $w_{q_i}^i$  must be 1 and we are done. The other two inequalities can be proved in the similar way with the help of two additional relations:  $x_{j-2h_i}^{i-1} \geq w_j^{i-1}$  and  $y_{j-2h_i}^{i-1} \geq x_j^{i-1}$ , which follows from the induction hypothesis.  $\square$

**Theorem 3.** *The output of Network 3 is top  $k$  sorted.*

*Proof.* The zip operation outputs its input vectors in the row-major order. By Eq. (3) of Lemma 3, we know that elements in the *out* sequence are dominated by the  $k$  largest elements in the output vectors of the main loop. From the order diagram given in Fig. 2 it follows that  $\langle y_{i-1}, \max(z_{i-1}, w_{j+1}), w_j, x_j \rangle$  dominates  $\langle y_i, z_i, \min(z_{i-1}, w_{j+1}), x_{i+1} \rangle$ , thus, after the sorting operations in lines 15–16, the values will appear in the row-major order. The two special cases, where the whole sequence of four elements is not available for the *sort*<sup>4</sup> operation, are covered by lines 17 and 18. If the vector  $\tilde{x}^i$  does not have the element with index  $k_4 + 1$ , then just 3 elements are sorted in line 17. If  $k \bmod 4 = 3$  then the element  $y_{k_4+1}$  is the last one in desired order, but the vector  $\tilde{z}^i$  does not have the element with index  $k_4 + 1$ , so the network must sort just 2 elements in line 18. Note that in the first  $\lfloor k/4 \rfloor$  rows we have  $4 \lfloor k/4 \rfloor$  elements of the top  $k$  ones, so the values of  $k - 4 \lfloor k/4 \rfloor$  leftmost elements in the row  $k_4 + 1$  should be corrected.  $\square$

## 4.2 4-Odd-Even Merging Networks

In this subsection the second merging algorithm for four columns is presented (Network 5). The input to the procedure is  $\langle \text{pref}(k_1, \bar{y}^1), \dots, \text{pref}(k_m, \bar{y}^m) \rangle$ , where each  $\bar{y}^i$  is the output of the recursive call in Network 2. Again, the goal is to put the  $k$  largest elements in top rows. It is done by splitting each input sequence into two parts, one containing elements of odd index, the other containing elements of even index. Odd sequences and even sequences are then recursively merged (lines 7–8). The resulting sequences are again split into odd and even parts, and combined using auxiliary Network 4 (lines 9–10). Lastly, the combine operation is used again (line 11) to get the top  $k$  sorted sequence.

Our network is the generalization of the classic Odd-Even Merging Network by Batchier [6]. Network 4 is the standard combine operation of the Odd-Even Merging Network, but with smaller number of comparators, since our network is the selection network. For more information on these classes of networks and to see examples, see [13].

**Definition 9.** *A binary sequence  $\bar{r}$  is top  $k'$  full if it is of the form  $1^{k'} \bar{r}'$ , where  $\bar{r}' \in \{0, 1\}^{|\bar{r}| - k'}$ .*

**Observation 3.** *Let  $K, k, l \in \mathbb{N}$  and  $K \geq k + l$  and  $0 \leq l - k \leq 2$ . If  $\bar{a}$  is top  $l$  full and  $\bar{b}$  is top  $k$  full then  $\text{oe\_combine}_K^{|\bar{a}| + |\bar{b}|}(\bar{a}, \bar{b})$  is top  $l + k$  full.*

*Proof.* If  $l \in \{k, k + 1\}$  or  $b_{k+1} = 1$ , then  $\text{oe\_combine}_K^{|\bar{a}| + |\bar{b}|}(\bar{a}, \bar{b})$  is top  $l + k$  full due to the zip operation in line 1 (notice that additional sorting is not

**Network 4**  $oe\_combine_k^s$ **Input:** A pair of sequences  $\langle \bar{x}, \bar{y} \rangle$ , where  $k \leq s = |\bar{x}| + |\bar{y}|$ .

- 1:  $\bar{z} \leftarrow \text{zip}(\bar{x}, \bar{y})$
- 2: **for all**  $i \in \{1, \dots, \lfloor \min(k, |\bar{z}| - 1)/2 \rfloor\}$  **do**
- 3:      $\text{sort}^2(z_{2i}, z_{2i+1})$
- 4: **return**  $\bar{z}$

needed). If  $l = k + 2$  and  $b_{k+1} = 0$ , then after the zip operation in line 1, the sequence  $\bar{z}$  is of the form  $1^{2k+1}01\{0, 1\}^*$ . Since  $K \geq k + l = 2k + 2$ , the elements  $\langle z_{2k+2}, z_{2k+3} \rangle = \langle 0, 1 \rangle$  will be sorted in line 3. Therefore  $\bar{z}$  will be of the form  $1^{2k+2}\{0, 1\}^*$ , so  $\bar{z}$  is top  $l + k$  full.  $\square$

**Network 5**  $4oe\_merge_k^s$ **Input:** A tuple of top  $k$  sorted sequences  $\langle \bar{w}, \bar{x}, \bar{y}, \bar{z} \rangle$ , where  $s = |\bar{w}| + |\bar{x}| + |\bar{y}| + |\bar{z}|$ ,  $|\bar{w}| \geq |\bar{x}| \geq |\bar{y}| \geq |\bar{z}|$  and  $k \geq 1$ .

- 1:  $k_1 = |\bar{w}|$ ;  $k_2 = |\bar{x}|$ ;  $k_3 = |\bar{y}|$ ;  $k_4 = |\bar{z}|$
- 2: **if**  $k_2 = 0$  **then return**  $\bar{w}$
- 3: **if**  $k_1 = 1$  **then**
- 4:      $\bar{a} \leftarrow \text{zip}(\bar{w}, \bar{x}, \bar{y}, \bar{z})$
- 5:     **return**  $\text{sort}^{|\bar{a}|}(\bar{a})$
- 6:  $sa = \lceil k_1/2 \rceil + \lceil k_2/2 \rceil + \lceil k_3/2 \rceil + \lceil k_4/2 \rceil$ ;  $sb = \lfloor k_1/2 \rfloor + \lfloor k_2/2 \rfloor + \lfloor k_3/2 \rfloor + \lfloor k_4/2 \rfloor$
- 7:  $\bar{a} \leftarrow 4oe\_merge_{\min(sa, \lfloor k/2 \rfloor + 2)}^{sa}(\bar{w}_{odd}, \bar{x}_{odd}, \bar{y}_{odd}, \bar{z}_{odd})$   $\triangleright$  Recursive calls.
- 8:  $\bar{b} \leftarrow 4oe\_merge_{\min(sb, \lfloor k/2 \rfloor)}^{sb}(\bar{w}_{even}, \bar{x}_{even}, \bar{y}_{even}, \bar{z}_{even})$
- 9:  $\bar{c} \leftarrow oe\_combine_{\lfloor k/2 \rfloor + 1}(\bar{a}_{odd}, \bar{b}_{odd})$
- 10:  $\bar{d} \leftarrow oe\_combine_{\lfloor k/2 \rfloor}(\bar{a}_{even}, \bar{b}_{even})$
- 11: **return**  $oe\_combine_k(\bar{c}, \bar{d})$   $\triangleright$  The output is top  $k$  sorted.

**Observation 4.** If  $\bar{x}$  is a sorted sequence, then  $|\bar{x}_{odd}|_1 - |\bar{x}_{even}|_1 \leq 1$ .

**Lemma 4.** Let  $k, k' \in \mathbb{N}$  and  $k' \leq k$ . If  $\langle \bar{w}, \bar{x}, \bar{y}, \bar{z} \rangle$  is a top  $k'$  sorted tuple such that  $k \leq s = |\bar{w}| + |\bar{x}| + |\bar{y}| + |\bar{z}|$  and  $|\bar{w}| \geq |\bar{x}| \geq |\bar{y}| \geq |\bar{z}|$ , then  $4oe\_merge_k^s(\bar{w}, \bar{x}, \bar{y}, \bar{z})$  is top  $k'$  sorted.

*Proof.* By induction on  $(k', s)$ . First we introduce the schema of the proof, as it has many base cases:

1. When  $k' \leq s = 1$  or  $k_1 = 1$ .
2. When  $k' = s$  and  $k_1 \geq 2$ .
3. When  $k' = 1$ .
4. When  $k' = 2$ .

After that we will prove the inductive step. Notice that we needed to include cases 2 and 4 in the base step, because inductive step is only viable when  $\lfloor k'/2 \rfloor + 2 \leq k'$ , which is when  $k' \geq 3$ .



*Ad. 1.* If  $k' \leq s = 1$ , then from  $k_1 \geq k_2 \geq k_3 \geq k_4$  we get that  $k_1 = 1$  and  $k_2 = 0$ . Therefore  $\bar{w}$  is the only non-empty input sequence and it consists of only one element, therefore it is sorted and the algorithm terminates on line 2. If  $k_1 = 1$ , then from  $k_1 \geq k_2 \geq k_3 \geq k_4$  we get that each input sequence has at most one element. Therefore using sorter of order at most 4 gives the desired result (lines 4–5).

*Ad. 2.* If  $k' = s$ , then  $k = s$ . Assume that  $k_1 \geq 2$ . We prove this case by induction on  $s$ . Base case is covered by (1). Take any  $s > 1$  and assume that for any  $s' < s$ , the lemma holds. Consider the execution of  $4oe\_merge_s^s(\bar{w}, \bar{x}, \bar{y}, \bar{z})$ . Each input sequence is top  $s$  sorted, therefore they are sorted. Which means that  $\langle \bar{w}_{odd}, \bar{x}_{odd}, \bar{y}_{odd}, \bar{z}_{odd} \rangle$  and  $\langle \bar{w}_{even}, \bar{x}_{even}, \bar{y}_{even}, \bar{z}_{even} \rangle$  are also sorted. Since  $\min(sa, \lfloor s/2 \rfloor + 2) = sa$ ,  $\min(sb, \lfloor s/2 \rfloor) = sb$ ,  $sa < s$  (because  $k_1 \geq 2$ ) and  $sb < s$  we can use the induction hypothesis to get that  $\bar{a}$  is top  $sa$  sorted and  $\bar{b}$  is top  $sb$  sorted. Since  $|\bar{a}| = sa$  and  $|\bar{b}| = sb$  we get that  $\bar{a}$  and  $\bar{b}$  are sorted. Using Observation 4 on the input sequences we also get that  $|\bar{a}|_1 - |\bar{b}|_1 \leq 4$ . Therefore sequences  $\bar{a}_{odd}, \bar{b}_{odd}, \bar{a}_{even}, \bar{b}_{even}$  are sorted and  $|\bar{a}_{odd}|_1 - |\bar{b}_{odd}|_1 \leq 2$  and  $|\bar{a}_{even}|_1 - |\bar{b}_{even}|_1 \leq 2$ . It is easy to check that  $|\bar{a}_{odd}|_1 + |\bar{b}_{odd}|_1 \leq \lceil sa/2 \rceil + \lceil sb/2 \rceil \leq \lceil sa/2 \rceil + \lfloor sb/2 \rfloor + 1 = \lceil s/4 \rceil + \lfloor s/4 \rfloor + 1 \leq \lfloor s/2 \rfloor + 1$ , (for  $s > 1$ ). Similarly we get  $|\bar{a}_{even}|_1 + |\bar{b}_{even}|_1 \leq \lfloor sa/2 \rfloor + \lfloor sb/2 \rfloor \leq \lceil sa/2 \rceil + \lfloor sb/2 \rfloor = \lceil s/4 \rceil + \lfloor s/4 \rfloor \leq \lfloor s/2 \rfloor$ , (for  $s > 1$ ). Therefore from Observation 3 we get that  $\bar{c}$  is top  $|\bar{a}_{odd}|_1 + |\bar{b}_{odd}|_1$  full and  $\bar{d}$  is top  $|\bar{a}_{even}|_1 + |\bar{b}_{even}|_1$  full. Also since  $\bar{a}_{odd}, \bar{b}_{odd}, \bar{a}_{even}, \bar{b}_{even}$  were sorted,  $\bar{c}$  and  $\bar{d}$  are also sorted. Using Observation 4 we get that  $|\bar{c}|_1 - |\bar{d}|_1 = |\bar{a}_{odd}|_1 + |\bar{b}_{odd}|_1 - |\bar{a}_{even}|_1 - |\bar{b}_{even}|_1 \leq 2$ . Also  $|\bar{c}|_1 + |\bar{d}|_1 \leq \lceil sa/2 \rceil + \lceil sb/2 \rceil + \lfloor sa/2 \rfloor + \lfloor sb/2 \rfloor = sa + sb = s$ . Therefore using Observation 3 we get that the sequence returned in line 11 is top  $|\bar{c}|_1 + |\bar{d}|_1$  full and it is sorted, since  $\bar{c}$  and  $\bar{d}$  were sorted. This completes the inductive step and this case.

*Ad. 3.* Let  $k \geq k' = 1$ . We prove this case by induction on  $s$ . Assume  $s > 1$  and  $k_1 \geq 2$  (the other cases are covered by (1)). Consider two sub-cases:

(i).  $|\bar{w} :: \bar{x} :: \bar{y} :: \bar{z}|_1 = 0$ . Therefore output of the algorithm is of the form  $0^*$ , so it is top  $k'$  sorted.

(ii).  $|\bar{w} :: \bar{x} :: \bar{y} :: \bar{z}|_1 > 0$ . Without loss of generality assume that  $|\bar{w}|_1 > 0$ , and because it is top  $k'$  sorted, we get that  $w_1 = 1$ . Because of that  $w_1^{odd} = 1$  and since  $k_1 \geq 2$ , we get that  $sa < s$ , so we can use induction hypothesis to get that  $\bar{a}$  is top  $\lceil k'/2 \rceil = 1$  sorted and  $a_1 = 1$ . From this we get that  $a_1^{odd} = 1$ , therefore  $c_1 = 1$ . From this we conclude that the output in line 11 is of the form  $1\{0, 1\}^*$ , so it is top  $k'$  sorted.

*Ad. 4.* Let  $k \geq k' = 2$ . Assume  $s > 2$  and  $k_1 \geq 2$  (the other cases are covered by (1) and (2)). From our assumptions  $\lceil k'/2 \rceil = \lfloor k'/2 \rfloor = 1$ . Therefore from case (3) we get that  $\bar{a}$  and  $\bar{b}$  are top 1 sorted. Notice that  $\lfloor k/2 \rfloor + 1 \geq 2$  and consider  $\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in \{\langle 0, 0 \rangle, \langle 1, 0 \rangle, \langle 1, 1 \rangle\}$ . Using Observation 3, in all possible cases  $\bar{c}$  is top 2 sorted (regardless of the value of  $a_3$ ) and  $\bar{d}$  is top 1 sorted. We can now consider all possible cases for values of  $c_1, c_2$  and  $d_1$  and using Observation 3 again, conclude that the sequence returned in line 11 is top  $2 = k'$  sorted.

We can finally prove the induction step. Assume  $s \geq k \geq k' > 2$  and  $k_1 \geq 2$ . Consider three cases:

(i) One of the input sequences (say  $\bar{w}$ ) is top  $k'$  full. Therefore  $\bar{w}_{odd}$  is top  $\lceil k'/2 \rceil$  full and  $\bar{w}_{even}$  is top  $\lfloor k'/2 \rfloor$  full. Also since  $s \geq k' > 2$  and  $k_1 \geq 2$  we get that  $sa < s$ ,  $sb < s$  and  $\lfloor k'/2 \rfloor + 2 \leq k'$ . Therefore we can use induction hypothesis to get that  $\bar{a}$  is top  $\lceil k'/2 \rceil$  full and  $\bar{b}$  is top  $\lfloor k'/2 \rfloor$  full. Therefore  $\bar{a}_{odd}$  is top  $\lceil \lceil k'/2 \rceil / 2 \rceil$  full,  $\bar{a}_{even}$  is top  $\lfloor \lceil k'/2 \rceil / 2 \rfloor$  full,  $\bar{b}_{odd}$  is top  $\lceil \lfloor k'/2 \rfloor / 2 \rceil$  full and  $\bar{b}_{even}$  is top  $\lfloor \lfloor k'/2 \rfloor / 2 \rfloor$  full. Let  $q = \lceil \lceil k'/2 \rceil / 2 \rceil + \lceil \lfloor k'/2 \rfloor / 2 \rceil$  and  $r = \lfloor \lceil k'/2 \rceil / 2 \rfloor + \lfloor \lfloor k'/2 \rfloor / 2 \rfloor$ . Notice that  $q \leq \lfloor k'/2 \rfloor + 1$  and  $r \leq \lfloor k'/2 \rfloor$  (for  $k' \geq 2$ ). Furthermore,  $0 \leq \lceil \lceil k'/2 \rceil / 2 \rceil - \lfloor \lfloor k'/2 \rfloor / 2 \rfloor \leq 1$  and  $0 \leq \lfloor \lceil k'/2 \rceil / 2 \rfloor - \lfloor \lfloor k'/2 \rfloor / 2 \rfloor \leq 1$ . Hence we can use Observation 3 to get that  $\bar{c}$  is top  $q$  full and  $\bar{d}$  is top  $r$  full. It is easy to check that  $0 \leq q - r \leq 2$  and  $q + r = k'$ , therefore we can use Observation 3 again and we can conclude that the last combine operation (line 11) will return top  $k'$  sorted sequence, therefore this case is done.

(ii) All input sequences are of the form  $1^j 0^*$ , where  $j < k'$ , and  $I = |\bar{w} :: \bar{x} :: \bar{y} :: \bar{z}|_1 \leq k'$ . Since  $s \geq k' > 2$  and  $k_1 \geq 2$  we get that  $sa < s$ ,  $sb < s$  and  $\lfloor k'/2 \rfloor + 2 \leq k'$ . Therefore using induction hypothesis we get that  $\bar{a}$  is of the form  $1^q 0^*$  and  $\bar{b}$  is of the form  $1^r 0^*$ , where  $q + r = I$ . Furthermore, applying Observation 4 to all input sequences we get that  $0 \leq q - r \leq 4$ . Which means that  $\bar{a}_{odd}, \bar{a}_{even}, \bar{b}_{odd}, \bar{b}_{even}$  are all sorted and of the form  $1^{\lceil q/2 \rceil} 0^*, 1^{\lfloor q/2 \rfloor} 0^*, 1^{\lceil r/2 \rceil} 0^*, 1^{\lfloor r/2 \rfloor} 0^*$  respectively, also  $0 \leq |\bar{a}_{odd}|_1 - |\bar{b}_{odd}|_1 = \lceil q/2 \rceil - \lceil r/2 \rceil \leq 2$  and  $0 \leq |\bar{a}_{even}|_1 - |\bar{b}_{even}|_1 = \lfloor q/2 \rfloor - \lfloor r/2 \rfloor \leq 2$ . Using Observation 3 we get that  $\bar{c}$  is top  $\lceil q/2 \rceil + \lceil r/2 \rceil$  full and  $\bar{d}$  is top  $\lfloor q/2 \rfloor + \lfloor r/2 \rfloor$  full. Moreover,  $0 \leq |\bar{c}|_1 - |\bar{d}|_1 = \lceil q/2 \rceil + \lceil r/2 \rceil - \lfloor q/2 \rfloor - \lfloor r/2 \rfloor \leq 2$ , therefore using Observation 3 again we conclude that the returned sequence (in line 11) is top  $q + r$  full, and since  $q + r = I < k'$ , then the returned sequence is of the form  $1^I 0^*$ , so it is also top  $k'$  sorted.

(iii) All input sequences are of the form  $1^j 0^*$ , where  $j < k'$ , and  $I = |\bar{w} :: \bar{x} :: \bar{y} :: \bar{z}|_1 > k'$ . Since  $s \geq k' > 2$  and  $k_1 \geq 2$  we get that  $sa < s$ ,  $sb < s$  and  $\lfloor k'/2 \rfloor + 2 \leq k'$ . Therefore we can use induction hypothesis to get that  $\bar{a}$  is top  $\lfloor k'/2 \rfloor + 2$  sorted and  $\bar{b}$  is top  $\lfloor k'/2 \rfloor$  sorted. Applying Observation 4 to all input sequences we get that  $0 \leq |\bar{a}|_1 - |\bar{b}|_1 \leq 4$ , in particular,  $|\bar{a}|_1 \geq |\bar{b}|_1$ . Let  $q = |a_{1 \dots \lfloor k'/2 \rfloor + 2}|_1$  and  $r = |b_{1 \dots \lfloor k'/2 \rfloor}|_1$ . Furthermore, either  $\bar{a}$  is top  $\lfloor k'/2 \rfloor + 2$  full or  $\bar{b}$  is top  $\lfloor k'/2 \rfloor$  full. Otherwise  $a_{\lfloor k'/2 \rfloor + 2} = 0$  and  $b_{\lfloor k'/2 \rfloor} = 0$ , which means that for each  $j \geq \lfloor k'/2 \rfloor + 2$  and  $j' \geq \lfloor k'/2 \rfloor$ ,  $a_j = 0$  and  $b_{j'} = 0$ . This implies that  $I \leq q + r \leq (\lfloor k'/2 \rfloor + 1) + (\lfloor k'/2 \rfloor - 1) \leq k'$ , a contradiction. Consider two cases: (A)  $\bar{b}$  is top  $\lfloor k'/2 \rfloor$  full. Since  $|\bar{a}|_1 \geq |\bar{b}|_1$ , then  $\bar{a}$  is also top  $\lfloor k'/2 \rfloor$  full. Furthermore, since  $I > k'$  it is true that  $\bar{a}$  is also top  $\lfloor k'/2 \rfloor + 1$ . This means that  $q + r \geq k'$ . For case (B) assume that  $\bar{a}$  is top  $\lfloor k'/2 \rfloor + 2$  full. If  $a_{\lfloor k'/2 \rfloor + 3} = 0$ , then since  $I > k'$  we get that  $\bar{b}$  is top  $\lfloor k'/2 \rfloor - 1$  full. This implies that  $q + r \geq k'$ . On the other hand, if  $a_{\lfloor k'/2 \rfloor + 3} = 1$ , then since  $|\bar{a}|_1 - |\bar{b}|_1 \leq 4$  we get that  $\bar{b}$  is top  $\lfloor k'/2 \rfloor - 1$  full, which also implies that  $q + r \geq k'$ . Therefore in all the cases  $q + r \geq k'$ . Notice that  $0 \leq \lceil q/2 \rceil - \lceil r/2 \rceil \leq 2$  and  $0 \leq \lfloor q/2 \rfloor - \lfloor r/2 \rfloor \leq 2$ . Using Observation 3 we get that  $\bar{c}$  is top  $\lceil q/2 \rceil + \lceil r/2 \rceil$  full and  $\bar{d}$  is top  $\lfloor q/2 \rfloor + \lfloor r/2 \rfloor$  full. Moreover,  $0 \leq \lceil q/2 \rceil + \lceil r/2 \rceil - \lfloor q/2 \rfloor - \lfloor r/2 \rfloor \leq 2$ , therefore using Observation 3 again we conclude that the returned sequence (in line 11) is top  $q + r$  full, and since  $q + r \geq k'$ , then the returned sequence is top  $k'$  sorted.  $\square$

## 5 Comparison of Selection networks

In this section we would like to estimate and compare the number of variables and clauses in encodings based on our algorithms to other encoding based on odd-even selection and pairwise selection proposed by Codish and Zazon-Ivry [9]. We start with counting how many variables and clauses are needed in order to merge 4 sorted sequences returned by recursive calls of 4-Wise Selection Network, Pairwise Cardinality Network, 4-Odd-Even Selection Network and Odd-Even Selection Network. Then, based on those values we prove that overall number of variables and clauses are almost always smaller when using 4-column encodings rather than 2-column encodings. In the next section we show that the new encodings are not just smaller, but also have better solving times in many benchmark instances.

To simplify the presentation we assume that  $k \leq n/4$  and both  $k$  and  $n$  are the powers of 4. We also omit the ceiling and floor function in the calculations, when it is convenient for us.

**Definition 10.** Let  $n, k \in \mathbb{N}$ . For given (selection) network  $f_k^n$  let  $V(f_k^n)$  and  $C(f_k^n)$  denote the number of variables and clauses used in the standard CNF encoding of  $f_k^n$ .

We remind the reader that a single 2-comparator uses 2 auxiliary variables and 3 clauses. In case of 3-comparator the numbers are 3 and 7, and for 4-comparator it's 4 and 15.

We begin by briefly introducing the Pairwise Cardinality Networks [9] that can be summed up by the following three-step recursive procedure (omitting the base case):

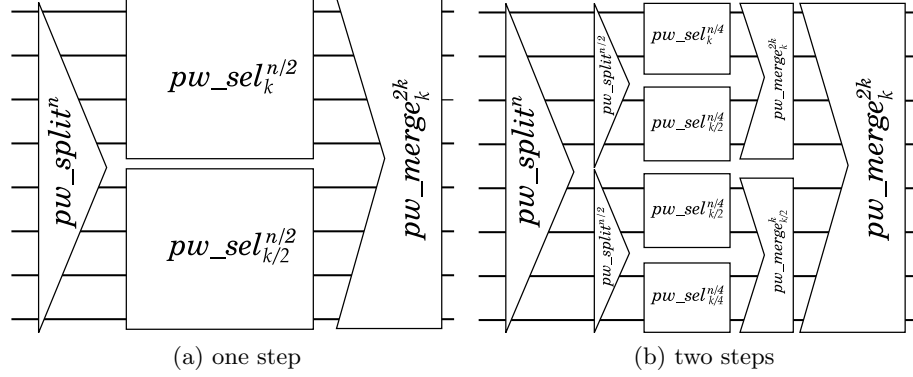
1. Split the input  $\bar{x} \in \{0, 1\}^n$  into two sequences  $\bar{x}^1$  and  $\bar{x}^2$  of equal size and order pairs, such that for each  $1 \leq i \leq n/2$ ,  $\bar{x}_i^1 \geq \bar{x}_i^2$ .
2. Recursively select top  $k$  sorted elements from  $\bar{x}^1$  and top  $k/2$  sorted elements from  $\bar{x}^2$ .
3. Merge the outputs of the previous step using a Pairwise Merging Network of order  $(2k, k)$  and output the top  $k$  elements.

The details of the above construction can be found in [9]. If we treat the splitting step as a network  $pw\_split^n$ , the merging step as a network  $pw\_merge_k^{2k}$ , then the number of 2-comparators used in the Pairwise Cardinality Network of order  $(n, k)$  can be written as:

$$|pw\_sel_k^n| = \begin{cases} |pw\_sel_k^{n/2}| + |pw\_sel_{k/2}^{n/2}| + \\ + |pw\_split^n| + |pw\_merge_k^{2k}| & \text{if } k < n \\ |oe\_sort^k| & \text{if } k = n \\ |max^n| & \text{if } k = 1 \end{cases} \quad (8)$$

One can check that Step 1 requires  $|pw\_split^n| = n/2$  2-comparators and Step 3 requires  $|pw\_merge_k^{2k}| = k \log k - k + 1$  2-comparators. The schema of

this network is presented in Figure 4. We want to count the number of variables and clauses used in merging 4 outputs of the recursive steps, therefore we expand the recursion by one level (see Figure 4b).



**Fig. 4.** Pairwise Cardinality Network

**Lemma 5.** *Let  $k \in \mathbb{N}$ . Then  $2V(pw\_merge_k^{2k}) + V(pw\_merge_{k/2}^k) = 5k \log k - 6k + 6$  and  $2C(pw\_merge_k^{2k}) + C(pw\_merge_{k/2}^k) = \frac{15}{2}k \log k - 9k + 9$ .*

*Proof.* The number of 2-comparator used is:

$$2|pw\_merge_k^{2k}| + |pw\_merge_{k/2}^k| = \frac{5}{2}k \log k - 3k + 3$$

Elementary calculation gives the desired result.  $\square$

We now count the number of variables and clauses for the 4-Wise Selection Network, again, disregarding the recursive steps.

**Lemma 6.** *Let  $k \in \mathbb{N}$ . Then  $V(4w\_merge_k^{4k}) = k \log k + \frac{7}{6}k - 5$ ,  $C(4w\_merge_k^{4k}) = \frac{15}{4}k \log k - \frac{33}{24}k - 10$ .*

*Proof.* We separately count the number of 2, 3 and 4-comparators used in the merger (Network 3). By the assumption that  $k \leq n/4$  we get  $|\bar{w}| = k$ ,  $|\bar{x}| = k/2$ ,  $|\bar{y}| = k/3$ ,  $|\bar{z}| = k/4$  and  $h_1 = k/2$ . We will consider iterations 1, 2 and 3 separately and then provide the formulas for the number of comparators for iterations 4 and beyond. Results are summarized in Table 1.

In the first iteration  $h_1 = k/2$ , which means that sets of  $j$ -values in the first two inner loops (lines 7–10 and 11–13) are empty. On the other hand,  $1 \leq j \leq \min(k_1 - h_1, k_2, h_1) = k/2$  (line 14), therefore  $k/2$  2-comparators are used. In fact it is true for every iteration  $i$  that  $\min(k_1 - h_i, k_2, h_i) = h_i = k/2^i$ . We note this fact in column 3 of Table 1 (the first term of each expression). For the next iterations we only need to consider the first and second inner loops of the algorithm.

$i$	$h_i$	#2-comparators	#3-comparators	#4-comparators
1	$\frac{k}{2}$	$\frac{k}{2}$	0	0
2	$\frac{k}{4}$	$\frac{k}{4} + \frac{k}{12}$	$\frac{k}{4}$	0
3	$\frac{k}{8}$	$\frac{k}{8}$	$\frac{k}{8}$	$\frac{5k}{24}$
$\geq 4$	$\frac{k}{2^i}$	$\frac{k}{2^i}$	$\frac{k}{2^i}$	$\frac{k}{4}$
Sum		$\frac{13}{12}k - 1$	$\frac{k}{2} - 1$	$\frac{1}{4}k \log k - \frac{13k}{24}$

**Table 1.** Number of comparators used in different iterations of Network 3

In the second iteration  $h_2 = k/4$ , therefore in the first inner loop only the condition in line 10 will hold, and only when  $j \leq k/3 - k/4 = k/12$ , hence  $k/12$  2-comparators are used. In the second inner loop the  $j$ -values satisfy condition  $1 \leq j \leq \min(k_2 - h_2, k_3, h_2) = k/4$ . Therefore the condition in line 12 will hold for each  $j \leq k/4$ , hence  $k/4$  3-comparators are used. In fact it is true for every iteration  $i \geq 2$  that  $\min(k_2 - h_i, k_3, h_i) = k/2^i$ , so the condition in line 12 will be true for  $1 \leq j \leq k/2^i$ . We note this fact in column 4 of Table 1. For the next iterations we only need to consider the first inner loop of the algorithm.

In the third iteration  $h_3 = k/8$ , therefore  $j$ -values in the first inner loop satisfy the condition  $1 \leq j \leq \min(k_3 - h_3, k_4) = 5k/24$  and the condition in line 8 will hold for each  $j \leq 5k/24$ , hence  $5k/24$  4-comparators are used.

From the forth iteration  $h_i \leq k/16$ , therefore for every  $1 \leq j \leq \min(k_3 - h_i, k_4) = k/4$  the condition in line 8 holds. Therefore  $k/4$  4-comparators are used.

What's left is to sum 2,3 and 4-comparators throughout  $\log k$  iterations of the algorithm. The results are presented in Table 1. Elementary calculation gives the desired result.  $\square$

Let  $V_{PCN} = 2V(pw\_merge_k^{2k}) + V(pw\_merge_{k/2}^k)$ ,  $C_{PCN} = 2C(pw\_merge_k^{2k}) + C(pw\_merge_{k/2}^k)$ ,  $V_{4W} = V(4w\_merge_k^{4k})$  and  $C_{4W} = C(4w\_merge_k^{4k})$ . Then the following corollary shows that using 4-column pairwise merging networks produces smaller encodings than their 2-column counterpart.

**Corollary 2.** *Let  $k \in \mathbb{N}$  such that  $k \geq 4$ . Then  $V_{4W} < V_{PCN}$  and  $C_{4W} < C_{PCN}$ .*

For the following theorem, note that  $V(4w\_split^n) = V(pw\_split^n) = n$ .

**Theorem 4.** *Let  $n, k \in \mathbb{N}$  such that  $1 \leq k \leq n/4$  and  $n$  and  $k$  are both powers of 4. Then  $V(4w\_sel_k^n) \leq V(pw\_sel_k^n)$ .*

*Proof.* Proof is by induction. For the base case, consider  $1 = k < n$ . It follows that  $V(4w\_sel_k^n) = V(pw\_sel_k^n) = V(max^n)$ . For the induction step assume that

for each  $(n', k') \prec (n, k)$  (in lexicographical order), where  $k \geq 4$ , the inequality holds, we get:

$$\begin{aligned}
V(4w\_sel_k^n) &= V(4w\_split^n) + \sum_{1 \leq i \leq 4} V(4w\_sel_{k/i}^{n/4}) + V(4w\_merge_k^{4k}) \\
&\quad \text{(by the construction of } 4w\_sel) \\
&\leq V(4w\_split^n) + \sum_{1 \leq i \leq 4} V(pw\_sel_{k/i}^{n/4}) + V(4w\_merge_k^{4k}) \\
&\quad \text{(by the induction hypothesis)} \\
&\leq V(pw\_split^n) + 2V(pw\_split^{n/2}) + \sum_{1 \leq i \leq 4} V(pw\_sel_{k/i}^{n/4}) \\
&\quad + 2V(pw\_merge_k^{2k}) + V(pw\_merge_{k/2}^k) \\
&\quad \text{(by Corollary 2 and because } V(4w\_split^n) < V(pw\_split^n) + 2V(pw\_split^{n/2})) \\
&\leq V(pw\_split^n) + 2V(pw\_split^{n/2}) + V(pw\_sel_k^{n/4}) + 2V(pw\_sel_{k/2}^{n/4}) \\
&\quad + V(pw\_sel_{k/4}^{n/4}) + 2V(pw\_merge_k^{2k}) + V(pw\_merge_{k/2}^k) \\
&\quad \text{(because } V(pw\_sel_{k/3}^{n/4}) \leq V(pw\_sel_{k/2}^{n/4})) \\
&= V(pw\_sel_k^n) \\
&\quad \text{(by the construction of } pw\_sel)
\end{aligned}$$

□

Now we will count how many variables and clauses are needed in order to merge 4 sorted sequences returned by recursive calls of Odd-Even Selection Network and 4-Odd-Even Selection Network, respectively. Two-column selection network using odd-even approach is presented in [9]. We briefly introduce this network with the following three-step recursive procedure (omitting the base case):

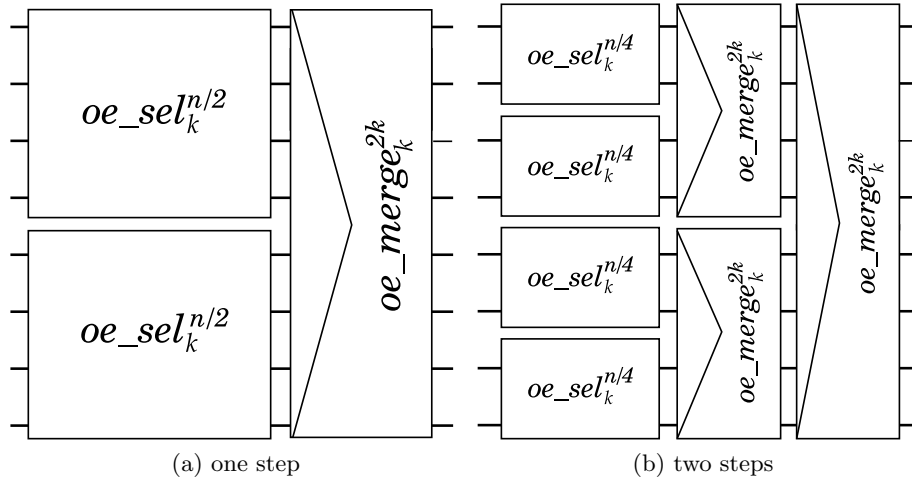
1. Split the input  $\bar{x} \in \{0, 1\}^n$  into two sequences  $\bar{x}^1 = \bar{x}_{odd}$  and  $\bar{x}^2 = \bar{x}_{even}$ .
2. Recursively select top  $k$  sorted elements from  $\bar{x}^1$  and top  $k$  sorted elements from  $\bar{x}^2$ .
3. Merge the outputs of the previous step using a Odd-Even Merging Network of order  $(2k, k)$  and output the top  $k$  elements.

If we treat the merging step as a network  $oe\_merge_k^{2k}$ , then the number of 2-comparators used in the Odd-Even Selection Network of order  $(n, k)$  can be written as:

$$|2oe\_sel_k^n| = \begin{cases} 2|2oe\_sel_k^{n/2}| + |2oe\_merge_k^{2k}| & \text{if } k < n \\ |oe\_sort_k^n| & \text{if } k = n \\ |max^n| & \text{if } k = 1 \end{cases} \quad (9)$$

One can check that Step 3 requires  $|2oe\_merge_k^{2k}| = k \log k + 1$  2-comparators. Overall number of 2-comparators was already calculated in [9].

**Lemma 7 ([9]).** *For  $k \leq n$  (both powers of two)  $2oe\_sel_k^n$  uses  $\frac{1}{4}n \log^2 k + \frac{3}{4}n \log k - k \log k$  2-comparators.*



**Fig. 5.** Pairwise Cardinality Network

The schema of this network is presented in Figure 5. Similarly to the previous case, in order to count the number of comparators used in merging 4 sorted sequences we need to expand the recursive step by one level (see Figure 5b).

**Lemma 8.**  $3V(2oe\_merge_k^{2k}) = 6k \log k + 6$ ,  $3C(2oe\_merge_k^{2k}) = 9k \log k + 9$ .

*Proof.* The number of 2-comparators used is:

$$3|2oe\_merge_k^{2k}| = 3k \log k + 3$$

Elementary calculation gives the desired result.  $\square$

Now we do the same counting for our 4-Odd-Even Selection Network based on Networks 2 and 5.

**Lemma 9.** Let  $k \in \mathbb{N}$ . Then  $V(4oe\_merge_k^{4k}) \leq 2k \log k + 16k - 4 \log k - 6$  and  $C(4oe\_merge_k^{4k}) \leq 3k \log k + 33k - 6 \log k - 9$ .

*Proof.* We separately count the number of 2 and 4-comparators used. We count the comparators in the merger (Network 5). By the assumption that  $k \leq n/4$  and that  $k$  is the power of 4 we get that  $|\bar{w}| = |\bar{x}| = |\bar{y}| = |\bar{z}| = k$ . This implies that  $s = 4k$  and  $sa = sb = 2k$ .

In the algorithm 4-comparators are only used in the base case (line 3–5). Furthermore number of 4-comparators is only dependent on the variable  $s$ . The solution to the following recurrence gives the sought number:  $\{A(4) = 1; A(s) = 2A(s/2), \text{ for } s > 4\}$ , which is equal to  $s/4 = k$ .

We now count the number of 2-comparators used. The combine operations in lines 9–11 uses  $(2k/2 + 1 + k)/2 \leq k + 1$  2-comparators. The total number of 2-comparators is then a solution to the following recurrence:

$$B(s, k) = \begin{cases} 0 & \text{if } s \leq 4 \\ B(s/2, k/2 + 2) + B(s/2, k/2) + k + 1 & \text{otherwise} \end{cases}$$

We claim that  $B(s, k) \leq k \log \frac{s}{2} - k - 2 \log s + \frac{3}{2}s + 1$ . This can be easily verified using induction. Applying  $s = 4k$  gives us the upper bound on number of 2-comparators used, which is  $k \log k + 6k - 2 \log k - 3$ .

Elementary calculation gives the desired result.  $\square$

Let  $V_{2OE} = 3V(oe\_merge_k^{2k})$ ,  $C_{2OE} = 3C(oe\_merge_k^{2k})$ ,  $V_{4OE} = V(4oe\_merge_k^{4k})$  and  $C_{4OE} = C(4oe\_merge_k^{4k})$ .

**Corollary 3.** *Let  $k \in \mathbb{N}$ . If  $k \geq 16$ , then  $V_{4OE} \leq V_{2OE}$ . If  $k \geq 64$ , then  $C_{4OE} \leq C_{2OE}$ .*

The corollary above does not cover all values of  $k$ . For the sake of the next theorem we set  $k = 4$  and compare values  $V(4oe\_sel_4^n)$  and  $V(2oe\_sel_4^n)$  in the following lemma. We do similar calculations for  $C(4oe\_sel_k^n)$  and  $C(2oe\_sel_k^n)$ , for  $k \in \{4, 16\}$ .

**Lemma 10.** *Let  $n \in \mathbb{N}$  such that  $n \geq 16$  and  $n$  is a power of 4. Then  $V(4oe\_sel_4^n) \leq V(2oe\_sel_4^n)$ .*

*Proof.* Applying  $k = 4$  to the formula in Lemma 7 gives  $\frac{5}{2}n - 8$  2-comparators and therefore  $V(2oe\_sel_4^n) = 5n - 16$ .

On the other hand, we calculate the value  $B(s, k)$  from Lemma 9 more accurately when  $k = 4$  to get accurate result for  $V(4oe\_merge_4^n)$  and, in consequence, for  $V(4oe\_sel_4^n)$ . First we rewrite the formula so it represents the number of variables used in  $4oe\_merge_k^n$ :

$$B^*(s, k) = \begin{cases} 4 & \text{if } s \leq 4 \\ B^*(s/2, \lfloor k/2 \rfloor + 2) + B^*(s/2, \lfloor k/2 \rfloor) + 4 \lfloor k/2 \rfloor + 2 & \text{otherwise} \end{cases}$$

The change is straightforward. Since  $s = 4k$ , we can calculate by hand that  $B^*(16, 4) = 42$ . The sought value is given by:

$$V(4oe\_sel_4^n) = \begin{cases} V(4oe\_merge_4^{16}) + 16 & \text{if } n = 16 \\ 4V(4oe\_sel_4^{n/4}) + V(4oe\_merge_4^{16}) & \text{otherwise} \end{cases}$$

In the first case we use one merger of order  $(16, 4)$  and 4 4-comparators. The second case is straightforward. Since  $V(4oe\_merge_4^{16}) = B^*(16, 4)$ , so the recursive formula above can be reduced into:

$$f(n) = \begin{cases} 58 & \text{if } n = 16 \\ 4f(n/4) + 42 & \text{otherwise} \end{cases}$$

for which the solution is  $f(n) = \frac{9}{2}n - 14$ . Obviously  $\frac{9}{2}n - 14 \leq 5n - 16$ , for  $n \geq 4$ , so we are done.  $\square$



**Theorem 5.** *Let  $n, k \in \mathbb{N}$  such that  $1 \leq k \leq n/4$  and  $n$  and  $k$  are both powers of 4. Then  $V(4oe\_sel_k^n) \leq V(2oe\_sel_k^n)$ .*

*Proof.* Proof is by induction. For the base case, consider  $1 = k < n$ . It follows that  $V(2oe\_sel_k^n) = V(4oe\_sel_k^n) = V(max^n)$ . The case  $n > k = 4$  is handled by Lemma 10. For the induction step assume that for each  $(n', k') \prec (n, k)$  (in lexicographical order), where  $k \geq 16$ , the inequality holds, we get:

$$\begin{aligned}
 V(4oe\_sel_k^n) &= 4V(4oe\_sel_k^{n/4}) + V(4oe\_merge_k^{4k}) \\
 &\quad \text{(by the construction of } 4oe\_sel) \\
 &\leq 4V(2oe\_sel_k^{n/4}) + V(4oe\_merge_k^{4k}) \\
 &\quad \text{(by the induction hypothesis)} \\
 &\leq 4V(2oe\_sel_k^{n/4}) + 3V(2oe\_merge_k^{2k}) \\
 &\quad \text{(by Corollary 3)} \\
 &= V(2oe\_sel_k^n) \\
 &\quad \text{(by the construction of } 2oe\_sel)
 \end{aligned}$$

□

## 6 Experimental Evaluation

As it was observed in [1], having a smaller encoding in terms of number of variables or clauses is not always beneficial in practice, as it should also be accompanied with a reduction of SAT-solver runtime. In this section we assess how our encodings based on the new family of selection networks affect the performance of a SAT-solver.

Our algorithms that encode CNF instances with cardinality constraints into CNFs were implemented as an extension of MINICARD ver. 1.1, created by Mark Liffiton and Jordyn Maglalang<sup>1</sup>. MINICARD uses three types of solvers:

- *minicard* - the core MINICARD solver with native AtMost constraints,
- *minicard\_encodings* - a cardinality solver using CNF encodings for AtMost constraints,
- *minicard\_simp\_encodings* - the above solver with simplification / preprocessing.

The main program in *minicard\_encodings* has an option to generate a CNF formula, given a CNFP instance (CNF with the set of cardinality constraints) and to select a type of encoding applied to cardinality constraints. Program run with this option outputs a CNF instance that consists of collection of the original clauses with the conjunction of CNFs generated by given method for each cardinality constraint. No additional preprocessing and/or simplifications are made. Authors of *minicard\_encodings* have implemented six methods to encode cardinality constraints and arranged them in one library called *Encodings.h*.

<sup>1</sup> See <https://github.com/liffiton/minicard>

Our modification of MINICARD is that we added implementations of encodings presented in this paper and put them in the library *Encodings\_MW.h*. Then, for each CNFP instance and each encoding method, we used MINICARD to generate CNF instances. After preparing, the benchmarks were run on a different SAT-solvers. Our extension of MINICARD, which we call KP-MINICARD, is available online<sup>2</sup>.

We use two SAT-solvers in this evaluation. The first one is the well known MINISAT (ver. 2.2.0) created by Niklas Eén and Niklas Sörensson<sup>3</sup>. The second SAT-solver is the GLUEMINISAT (ver. 2.2.8), by Hidetomo Nabeshima, Koji Iwanuma and Katsumi Inoue<sup>4</sup>. All experiments were carried out on the machines with Intel(R) Core(TM) i7-2600 CPU @ 3.40GHz.

Detailed results are available online<sup>5</sup>. We publish spreadsheets showing running time for each instance, speed-up/slow-down tables for our encodings, number of time-outs met and total running time.

**Encodings:** From this paper we choose two multi-column selection networks for evaluation:

- **4WISE** - 4-column selection network based on pairwise approach (Networks 1 and 3),
- **4OE** - 4-column odd-even selection network based on Networks 2 and 5.

We compare our encodings to some others found in the literature. We consider the Pairwise Cardinality Networks [9] to rival our 4-column pairwise selection network. We also consider a solver called MINISAT+<sup>6</sup> which implements techniques to encode Pseudo-Boolean constraints to propositional formulas [10]. Since cardinality constraints are a subclass of Pseudo-Boolean constraints, we can measure how well the encodings used in MINISAT+ perform, compared with our methods. The solver chooses between three techniques to generate SAT encodings for Pseudo-Boolean constraints. These convert the constraint to: a BDD structure, a network of binary adders, a network of sorters. The network of adders is the most concise encoding, but it has poor propagation properties and often leads to longer computations than the BDD based encoding. The network of sorters is the implementation of classic odd-even (2-column) sorting network by Batcher [6]. Calling the solver we can choose the encoding with one of the parameters: *-ca*, *-cb*, *-cs*. By default, MINISAT+ uses the so called **Mixed** strategy, where program chooses which method (*-ca*, *-cb* or *-cs*) to use in the encodings, and this depends on size of the input and memory restrictions. We don't include **Mixed** strategy in the results, as the evaluation showed that it performs almost the same as *-cb* option. The generated CNFs were written to files with the option *-cnf=<file>*.

To sum up, here are the competitors' encodings used in this evaluation:

<sup>2</sup> See <https://github.com/karpiu/kp-minicard>

<sup>3</sup> See <https://github.com/niklasso/minisat>

<sup>4</sup> See <http://glueminisat.nabelab.org/>

<sup>5</sup> See <http://www.ii.uni.wroc.pl/%7ekarp/sat/2017.html>

<sup>6</sup> See <https://github.com/niklasso/minisatp>

- **PCN** - the Pairwise Cardinality Networks (our implementation)
- **CA** - encodings based on Binary Adders (from MINISAT+)
- **CB** - encodings based on Binary Decision Diagrams (from MINISAT+)
- **CS** - the Odd-Even Sorting Networks (from MINISAT+)

Additionally, encodings **4WISE**, **4OE** and **PCN** were extended, following the idea presented in [1], where authors use Direct Cardinality Networks in their encodings for sufficiently small values of  $n$  and  $k$ . Values of  $n$  and  $k$  for which we substitute the recursive calls with Direct Cardinality Network were selected based on our knowledge and some experiments.

Solver MINISAT+ have been slightly modified, namely, we fixed several bugs such as the one reported in the experiments section of [5].

**Benchmarks:** We used the following sets of benchmarks:

**1. MSU4 suite:** A set consisting of about 14000 benchmarks, each of which contains a mix of CNF formula and multiple cardinality constraints. This suite was created from a set of MaxSAT instances reduced from real-life problems, and then it was converted by the implementation of *msu4* algorithm [14]. This algorithm reduces a MaxSAT problem to a series of SAT problems with cardinality constraints. The MaxSAT instances were taken from the Partial Max-SAT division of the Third Max-SAT evaluation<sup>7</sup>. We perform experiments for this benchmarks using MINISAT.

**2. PB15 suite:** A set of benchmarks from the Pseudo-Boolean Evaluation 2015<sup>8</sup>. One of the categories of the competition was *DEC-LIN-32-CARD*, which contains 2289 instances – we use these in our evaluation. Every instance is a set of cardinality constraints. This set of benchmarks were evaluated using GLUEMINISAT.

**Results:** The time-out limit in the SAT-solvers was set to 600 seconds in case of MSU4 suite, and 1800 seconds for PB15 suite. When comparing two encodings we only considered instances for which at least one achieved the SAT-solver runtime of at least 10% of the time-out limit. All other instances were considered trivial, and therefore were not included in the results. We also filtered out the instances for which relative percentage deviation of the running time of encoding **A** w.r.t the running time of encoding **B** was less than 10% (and vice-versa), i.e.,  $|(t(A, I) - t(B, I))| / \min(t(A, I), t(B, I)) \leq 0.1$ , where  $t(E, I)$  is the time in which the SAT-solver terminated given a CNF generated from the instance  $I$  using encoding  $E$ .

Tables 2 and 3 present speed-up and slow-down factors for encodings **4OE** and **4WISE** w.r.t all other encodings. For PB15 suite we only show speed-up/slow-down of **4OE**, since from the first batch of tests (on MSU4 suite) we can conclude that it is the superior encoding. Explanation of how to read the tables now follows. Consider the comparison of encoding **A** w.r.t encoding **B**. In the speed-up section, **TO** indicates the number of instances run with encoding

<sup>7</sup> See <http://www.maxsat.udl.cat/08/index.php?disp=submitted-benchmarks>

<sup>8</sup> See <http://pbeva.computational-logic.org/>

	4OE speed-up						4OE slow-down					
	TO	4.0	2.0	1.5	1.1	Total	TO	4.0	2.0	1.5	1.1	Total
PCN	54	73	1	6	9	143	1	6	0	2	4	13
4WISE	26	48	11	5	4	94	2	7	4	3	4	20
CA	840	1114	0	6	4	1964	2	3	1	1	3	10
CB	100	187	0	7	3	297	3	6	1	4	2	16
CS	53	73	0	2	4	132	2	17	0	2	0	21

	4WISE speed-up						4WISE slow-down					
	TO	4.0	2.0	1.5	1.1	Total	TO	4.0	2.0	1.5	1.1	Total
PCN	30	35	16	8	12	101	1	7	6	2	6	22
4OE	2	7	4	3	4	20	26	48	11	5	4	94
CA	816	1083	13	7	8	1927	2	3	4	1	3	13
CB	86	154	23	11	6	280	13	18	5	2	4	42
CS	35	50	6	2	5	98	8	34	5	3	3	53

**Table 2.** Comparison of encodings in terms of SAT-solver runtime on MSU suite. We count number of benchmarks for which **4OE** and **4WISE** showed speed-up or slow-down factor with respect to different encodings.

**B** that ended as time-outs but were solved while run with encoding **A**. The **TO** value in the slow-down section means that the opposite is true. Column headers with numbers indicate speed-up (slow-down) factors for the encoding **A**, for example, instances counted in column 1.5 are those for which  $2.0 \cdot t(A, I) \geq t(B, I) > 1.5 \cdot t(A, I)$  for speed-up, and  $2.0 \cdot t(A, I) \leq t(B, I) < 1.5 \cdot t(A, I)$  for slow-down. In case of factor 4.0 the other coefficient is  $\infty$ .

From the evaluation we can conclude that the best performing encoding is **4OE**, on both MSU4 and PB15 suites. On MSU4 suite (Table 2), the superiority is apparent, as our encoding achieve significant speed-up factor w.r.t all other encodings. The runner-up encoding is **4WISE**, which performs worse than **4OE**, but still beats all other encodings. This is also reflected in the total running times and number of time-outs met over all instances – those values are presented in Table 4. We see that on MSU4 suite, SAT-solver finished twice as fast using encoding **4OE** rather than **CS**, and solved almost all instances in given time. Similar observation can be made for **4WISE** w.r.t **PCN**, where our encoding has about 18 000 seconds (5 hours) smaller total time and 75% less time-outs. This shows that using 4-column selection networks is more desirable than using 2-column selection/sorting networks for encoding cardinality constraints. Encodings **CA** and **CB** had the worst performance on MSU4 suite.

As for the results on PB15 suite, we see that the total running times and time-outs are similar (Table 4) for all encodings. This is due to the fact that PB15 suite contains a lot of hard instances and a lot of trivial instances, so the true competition boils down to a few medium-sized instances. Still, encoding **4OE** is the clear winner, having finished computations about 20 000 seconds

	4OE speed-up						4OE slow-down					
	TO	4.0	2.0	1.5	1.1	Total	TO	4.0	2.0	1.5	1.1	Total
PCN	4	4	1	4	11	24	0	0	2	4	8	14
4WISE	2	0	2	4	9	17	0	0	3	3	10	16
CA	10	13	32	13	20	88	2	2	6	5	15	30
CB	8	5	15	7	18	53	6	0	5	14	7	32
CS	15	10	17	14	19	75	6	1	5	8	17	37

**Table 3.** Comparison of encodings in terms of SAT-solver runtime on PB15 suite. We count number of benchmarks for which **4OE** showed speed-up or slow-down factor with respect to different encodings.

		4OE	4WISE	CS	PCN	CB	CA
<b>MSU4</b>	Total time	25319	44978	52284	62695	102894	695003
	Time-outs	16	40	67	69	113	854
<b>PB15</b>	Total time	2291394	2292065	2311042	2294726	2301762	2312199
	Time-outs	1240	1242	1249	1244	1242	1248

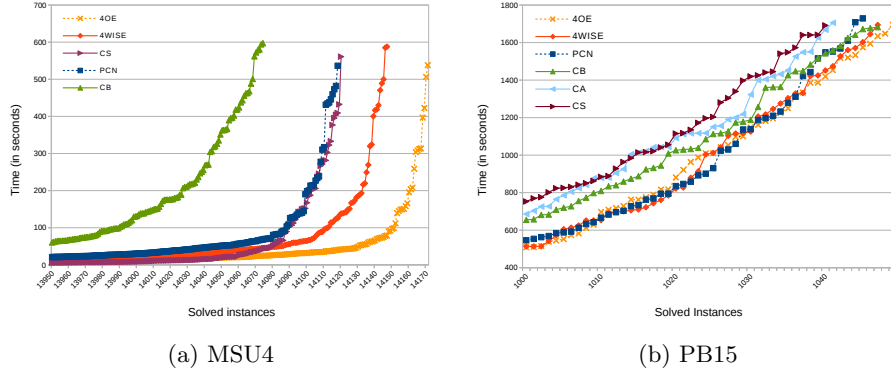
**Table 4.** Total running time (in seconds) of all instances and total number of time-outs.

(5.5 hours) faster than **CS**. Encoding **4WISE** performs similar to **4OE**, with only about 10 minutes gap in the total running time, but it is the latter that solved the most number of instances. Encoding **4OE** also outperforms all other encodings in terms of speed-up, which is presented in Table 3.

In Figure 6 we present two cactus plots, where x-axis gives the number of solved instances and the y-axis the time needed to solve them (in seconds) using given encoding. Results for MSU4 suite are in Figure 6a and for PB15 suite in Figure 6b. Notice that we did not include the **CA** encoding in the first plot, as it was not competitive to the other encodings. From the plots we can see again that the **4OE** encoding outperforms all other encodings.

## 7 Conclusions

In this paper we presented a family of multicolumn selection networks based on odd-even and pairwise approach, that can be used to encode cardinality constraints. We showed detailed constructions where the number of columns is equal to 4 and showed that their CNF encodings are smaller than their 2-column counterparts. We extended the encodings by applying the Direct Cardinality Networks of [1] for sufficiently small input. The new encodings were compared with the selected state-of-art encodings based on comparator networks, adders and binary decision diagrams. The experimental evaluation shows that the new encodings yield significant speed-ups in the SAT-solver performance.



**Fig. 6.** Number of solved instances of MSU4 suite and PB15 suite in given time.

Developing new methods to encode cardinality constraints based on comparator networks is important from the practical point of view. Using such encodings give an extra edge in solving optimization problems for which we need to solve a series of problems that differ only in that a bound on cardinality constraint  $x_1 + \dots + x_n \leq k$  becomes tighter, i.e., by decreasing  $k$  to  $k'$ . In this setting we only need to add one more clause  $\neg y_{k'}$ , and the computation can be resumed while keeping all the previous clauses untouched. This operation is allowed because if a comparator network is a  $k$ -selection network, then it is also a  $k'$ -selection network, for any  $k' < k$ . This property is called *incremental strengthening* and most state-of-art SAT-solvers provide an interface for doing this.

## References

1. Abío, I., Nieuwenhuis, R., Oliveras, A., Rodríguez-Carbonell, E.: A Parametric Approach for Smaller and Better Encodings of Cardinality Constraints. In: C. Schulte, (ed), Principles and Practice of Constraint Programming - CP 2013, LNCS, vol. 8124, pp. 80–96. Springer Heidelberg, (2013).
2. Anbulagan, Grastein, A.: Importance of Variables Semantic in CNF Encoding of Cardinality Constraints. In: V. Buitko and J. C. Beck, (ed), Eighth Symposium on Abstraction, Reformulation, and Approximation, SARA'09. AAAI, 2009.
3. Asín, R., Nieuwenhuis, R., Oliveras, A., Rodríguez-Carbonell, E.: Cardinality networks: a theoretical and empirical study. Constraints, 16(2):195–221, (2011).
4. Asín, R., Nieuwenhuis, R.: Curriculum-based course timetabling with SAT and MaxSAT. Annals of Operations Research, 218(1):71–91, (2014).
5. Aavani, A., Mitchell, D.G., Ternovska, E.: New encoding for translating pseudo-Boolean constraints into SAT. In: Frisch, A.M., Gregory, P. (eds.) SARA, AAAI (2013).
6. K. E. Batchier.: Sorting networks and their applications. In: Proc. of the April 30–May 2, 1968, Spring Joint Computer Conference, AFIPS '68 (Spring), pp. 307–314, ACM, New York, NY, USA, (1968).

7. K. E. Batchier, Lee, D.: A Multiway Merge Sorting Network. In: IEEE Transactions on Parallel and Distributed Systems, Vol. 6, No. 2, February 1995, pp. 211–215.
8. Biere, A., Cimatti, A., Clarke, E., Zhu, Y.: Symbolic Model Checking without BDDs. In: Proc. of 5th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'99), LNCS vol. 1579, pp. 193–207, Springer Heidelberg (1999).
9. Codish, M., Zazon-Ivry, M.: Pairwise cardinality networks. In: E. Clarke and A. Voronkov, (eds), Logic for Programming, Artificial Intelligence, and Reasoning, LNCS vol. 6355, pp. 154–172. Springer Heidelberg (2010).
10. Eén, N., Sörensson, N.: Translating pseudo-boolean constraints into sat. Journal on Satisfiability, Boolean Modeling and Computation, 2:1–26, (2006).
11. Gao, Q., Liu, Z., Zhao, L.: An efficient multiway merging algorithm. Science in China Series E: Technological Sciences, vol. 41:5, October 1998, Science in China Press, 1998.
12. Karpiński, M., Piotrów, M.: Smaller Selection Networks for Cardinality Constraints Encoding. In: G. Pesant, (ed), Principles and Practice of Constraint Programming - CP 2015, LNCS, vol. 9255, pp. 210–225. Springer International Publishing, 2015.
13. Knuth, D. E.: The Art of Computer Programming, Volume 3: (2Nd Ed.) Sorting and Searching. Addison Wesley Longman Publishing Co., Inc., Redwood City, CA, USA, (1998).
14. Marques-Silva, J., Planes, J.: Algorithms for Maximum Satisfiability using Unsatisfiable Cores. In: 2008 Conference on Design, Automation and Test in Europe Conference, DATE'08, pp. 408–413. IEEE Computer Society, 2008.
15. Parberry, I.: The pairwise sorting network. Parallel Processing Letters, 2:205–211, (1992).
16. Schutt, A., Feydy, T., Stuckey, P., Wallace, M.: Why cumulative decomposition is not as bad as it sounds. In: I. Gent, (ed), Principles and Practice of Constraint Programming - CP 2009, LNCS, vol. 5732, pp. 746–761. Springer Heidelberg, (2009).